Aurelian Claudiu VOLF

Structuri algebrice şi aplicaţii

Universitatea „Al. I Cuza" Iaşi

-2004-

(ultima modificare: 14 martie 2012)

Cuprins

Către cititor

Acest curs poate fi citit de un absolvent al anului I al Facultății de Matematică. Sînt presupuse cunoscute: noțiuni generale despre structuri algebrice (monoid, grup, inel, corp), construcția grupului factor, a inelului factor, noțiuni de bază despre spații vectoriale, matrice, polinoame, noțiuni elementare despre grupurile de permutări, aritmetica elementară a cardinalelor. Există un număr relativ mare de cărți şi cursuri în literatura matematică românească în care se tratează aceste lucruri. Unele direcții de aprofundare sînt indicate prin referințe bibliografice.

Parcurgerea unui text matematic este un proces *activ* prin excelență. În primul rînd, toate definițiile nou introduse trebuie sa capete rapid un suport intuitiv şi să fie legate de noțiunile deja cunoscute prin căutarea de exemple (şi contraexemple) de obiecte care să satisfacă definițiile. În plus, cititorul trebuie să *verifice* pe cazuri concrete şi să *demonstreze* afirmațiile din text. În particular, toate aparițiile unor fraze de tipul „se verifică uşor că …", „evident, …", … sînt o invitație la demonstrarea efectivă a afirmațiilor respective. Aceste exerciții intelectuale sînt un pas indispensabil spre asimilarea conceptelor şi tehnicilor introduse şi, totodată, o verificare a înțelegerii de către cititor a textului.

Paragrafele care au o bară la stînga sînt foarte importante pentru înțelegerea textului. Dacă merită reținută doar o singură frază dintr-o anumită secțiune, aceasta ar trebui să fie fraza marcată în acest mod.

Peste tot, în text:

- $|A|$ desemnează cardinalul mulțimii A (numărul elementelor lui A, dacă A este finită).
- $x := y$ înseamnă „x este egal prin definiție cu y" (unde y este deja definit) sau „notăm pe y cu x".
- □ marchează sfîrşitul sau absența unei demonstrații.

Prefață

Matematica are o reputație de disciplină aridă, abstractă, greu de asimilat, cu aplicabilitate restrînsă. De multe ori, cei care o studiază – de voie sau de nevoie – (își) pun întrebări de genul „la ce folosesc toate aceste definiții, notații, axiome, teoreme, … ?”. Dintre ramurile matematicii, algebra excelează în această direcție, în special algebra „abstractă” (sau „axiomatică”, sau încă „modernă”), care se ocupă de *structurile algebrice*.

De unde provine această reputație? Convingerea noastră este că ea se formează din experiența contactelor cu algebra din cursul gimnaziului şi liceului. Adesea, însuşi profesorul de matematică nu este foarte convins de utilitatea studiului anumitor noțiuni şi, în consecință, transmite elevilor doar o imagine formală şi seacă, din care motivațiile, exemplele şi aplicațiile sînt neglijate sau absente cu totul (uneori este „de vină” volumul mare de cunoştințe ce trebuie predat). Doar o cunoaştere aprofundată a conceptelor, care nu are cum să fie cantonată la nivelul unui manual de liceu, poate duce la conceperea unor lecții atractive, în care noțiunile nu sînt introduse în mod artificial, ci sînt însoțite permanent de exemple şi aplicații.

Unul din scopurile rîndurilor ce urmează este de a aduce argumente în sprijinul ideii că structurile algebrice, departe de a fi creații teoretice şi auto-suficiente, au apărut în mod natural, au un rol determinant în fundamentarea, simplificarea şi unificarea matematicii şi au aplicații consistente în practică şi în matematica însăşi.

Un alt scop al lucrării este de a oferi profesorilor de matematică un material care să arate că algebra este apropiată de realitate şi să îi convingă de frumusețea şi aplicabilitatea ei. De aceea, s-a avut în vedere şi latura didactică, punîndu-se accentul pe noțiunile care au legătură directă cu matematica studiată în învățămîntul preuniversitar.

Lucrarea se adresează studenților Facultăților de Matematică, profesorilor de matematică şi, în general, oricărui cititor interesat de algebră.

Titlul acestei lucrări face referire la Algebră. *Ce este însă algebra?* Încercăm să dăm un răspuns la această întrebare, după o argumentație a lui I.R. Shafarevich (KOSTRIKIN, SHAFAREVICH [1990]), care reia o idee a lui Hermann Weyl [1].

[1] Matematician german (1885-1955).

În procesul de cunoaştere a lumii fizice sînt esențiale procedee de *măsurare* şi de *structurare*, care permit ca impresiile subiective ale indivizilor umani să fie traduse în entități obiective, cel mai adesea în *numere*. Aceste entități, cu toate că nu redau integral experiența subiectivă, pot fi păstrate şi transmise nealterate. Mai mult, cu rezultatele măsurătorilor se pot face diverse *operații* (mai general, se pot *structura*), în scopul extragerii de noi informații, de a face predicții etc. Spre exemplu, structura matematică $\mathbb{N}$ a *numerelor naturale* este adecvată măsurării „mărimii" mulțimilor finite (făcînd abstracție de natura elementelor lor). *Numerele raționale*[2] au fost construite din motive evidente de măsurare a diverselor „mărimi fracționare", dar s-au dovedit incapabile de a măsura obiecte geometrice simple, cum este diagonala unui pătrat de latură 1. Astfel a apărut necesitatea construcției *numerelor iraționale*[3] şi, ulterior, a *numerelor reale*. *Numerele complexe* au avut o geneză asemănătoare, între altele din nevoia de a rezolva ecuații algebrice care nu au soluții reale. S-au imaginat şi alte extinderi ale conceptului de număr (*numerele cardinale* şi *numerele ordinale* sînt generalizări ale numerelor naturale; *cuaternionii* generalizează numerele complexe etc.).

Structura matematică $\mathbb{R}$ (corpul total ordonat al numerelor reale) este folosită pentru exprimarea multor mărimi fizice (lungimi, intensități, …). Cu ajutorul mulțimilor numerice (cel mai adesea $\mathbb{R}$) se pot construi structuri care pot măsura (un termen mai adecvat ar fi *coordonatiza*) multe obiecte şi fenomene. De pildă, spațiul liniar $\mathbb{R}^3$ modelează (cu ajutorul coordonatelor carteziene) *spațiul fizic*.

Extinderile succesive ale conceptului de număr (mai bine zis, construcțiile de structuri numerice din ce în ce mai largi) nu pot însă fi adecvate tuturor nevoilor de coordonatizare care pot apărea. De exemplu, „măsurarea" *simetriei* figurilor plane este cel mai bine realizată prin structura algebrică de *grup*: fiecărei figuri i se ataşează grupul său de simetrie (format din acele izometrii ale planului care invariază figura dată). Clasificarea *cristalelor* se realizează tot cu ajutorul grupurilor lor de simetrie. În mecanica cuantică, *spațiile Hilbert complexe* descriu sistemele cuantice: o stare a unui sistem cuantic este identificată cu un vector de normă 1 într-un astfel de spațiu.

Un alt exemplu este dat de *curbele plane*: o *curbă ireductibilă* C în $\mathbb{R}^2$ este mulțimea punctelor (x, y) din plan care satisfac ecuația $F(x, y) = 0$, unde $F \in \mathbb{R}[X, Y]$ este un polinom ireductibil fixat. Se presupune că curba C are o infinitate de puncte (se exclud deci curbe de tipul $x^2 + y^2 = 0$, care conține un singur punct). Atunci curbei C (polinomului F) i se asociază *corpul funcțiilor raționale pe C*, care în limbaj algebric modern poate fi descris ca fiind corpul de fracții al inelului integru $\mathbb{R}[X, Y]/(F)$. Acest corp reflectă proprietăți geometrice importante ale curbei C. În plus, prin schimbarea coordonatelor în care exprimăm ecuația curbei C, polinomul F se schimbă, însă noul corp al funcțiilor raționale este izomorf cu cel inițial. Iată

[2] De la *ratio*, care înseamnă raport (în latină).
[3] Denumirea de număr *irațional* provine de la faptul că acel număr nu poate fi exprimat ca un raport (*ratio*).

un exemplu de proprietate a curbei care este reflectată în structura algebrică a corpului funcțiilor raționale pe curbă. Curbele care pot fi parametrizate prin funcții raționale (adică există două funcții raționale $f, g : \mathbb{R} \to \mathbb{R}$ astfel încît $F(f(t), g(t)) = 0$ pentru toți t, cu excepția unui număr finit și $\forall(x, y)$ cu $F(x, y) = 0$ (cu excepția unui număr finit), $\exists t \in \mathbb{R}$ cu $(x,y) = (f(t), g(t)))$ sînt caracterizate de faptul că li se asociază un corp izomorf cu $\mathbb{R}(t)$ (corpul fracțiilor raționale cu coeficienți reali). Desigur, această construcție poate fi generalizată la alte corpuri decît $\mathbb{R}$ şi dimensiuni mai mari decît 2.

Se poate concluziona că:

În studiul obiectelor fizice sau abstracte apare nevoia de măsurare (coordonatizare) a fenomenelor sau a anumitor proprietăți ale obiectelor. Procesul de coordonatizare asociază fiecărui obiect (fenomen, proprietate…) o structură matematică (grup, inel, corp, spațiu Hilbert…), care descrie, total sau parțial, obiectul respectiv sau unele caracteristici ale sale.

Aceste considerații conduc la enunțarea următoarei descrieri de natură generală - şi inerent vagă - a Algebrei :

Obiectul de studiu al Algebrei este construcția şi studiul structurilor matematice apărute în acest mod.

I. Logică, mulțimi, axiome

Includerea capitolului privind logica şi teoria mulțimilor porneşte de la premisa că un profesor de matematică nu se poate limita la punctul de vedere al unui manual de liceu, fiind necesară o viziune mai profundă asupra acestor tematici.

Mulțimile apar ca obiecte matematice foarte devreme în învățămîntul modern, sub o formă intuitivă (în varianta teoriei naive a mulțimilor). Este exclusă o tratare axiomatică a teoriei mulțimilor la nivel preuniversitar; totuşi, un profesor de matematică trebuie să fie familiarizat cu conceptele ei de bază şi să înțeleagă utilitatea, necesitatea şi mecanismele teoriei axiomatice a mulțimilor.

Teoria modernă a mulțimilor începe odată cu lucrarea „Teoria rațională a infinității" a lui Georg Cantor[4], în care se manevrează liber *mulțimile infinite* şi se dezvoltă o tehnică de măsurare a lor (teoria cardinalelor). Pînă la Cantor, matematicienii adoptau punctul de vedere al filozofilor Greciei antice: există noțiunea de *infinit actual* (o infinitate de obiecte concepute ca existînd simultan) şi cea de *infinit potențial* (o mulțime sau o mărime finită, dar care se poate mări oricît de mult). Filozoful Zenon, prin faimoasele sale aporii (paradoxuri) a atras atenția asupra consecințelor absurde care par să apară introducînd infinitul actual în raționamente. Se considera de aceea că infinitul actual nu este accesibil intuiției şi doar infinitul potențial poate fi folosit în gîndirea matematică.

Cantor are meritul de a fi spart această barieră mentală şi de a fi încercat să „numere infinitul". El a avut ideea de a compara mulțimile (finite sau nu) cu ajutorul *funcțiilor bijective*: două mulțimi sînt „la fel de mari" (echipotente) dacă există o bijecție între ele. Cantor a obținut rezultate precum: $\mathbb{N}$ este echipotent cu $\mathbb{Q}$ şi cu mulțimea numerelor algebrice (numerele complexe care sînt rădăcini ale unui polinom nenul cu coeficienți raționali). Deja aceste afirmații nu sînt în acord cu percepția obişnuită şi arată că uneori „partea este la fel de mare ca şi întregul". A mai arătat că $\mathbb{N}$ nu este echipotent cu $\mathbb{R}$; în general, o mulțime A nu este echipotentă cu mulțimea părților sale $\mathcal{P}(A)$. Există, deci, mai multe tipuri de infinitate. Alte rezultate contrazic şi mai mult simțul comun: există tot atîtea puncte pe un segment cîte sînt pe o dreaptă sau în întregul plan sau în întregul spațiu!

---

[4] Georg Ferdinand Ludwig Philipp Cantor (1845-1918), matematician german.

În cadrul teoriei lui Cantor a mulţimilor (astăzi numită „naivă”), prin *mulţime* se înţelege o colecţie (un ansamblu, un set) de obiecte distincte (*elementele* mulţimii) bine determinată şi considerată ca o entitate. Georg Cantor spunea *„Unter eine Menge verstehen wir jede Zusammenfassung **M** von bestimmten Wohlunterschiedenen Objekten **m** unseres Denkens zu einem Ganzen“*: „Prin *mulţime* înţelegem orice grupare într-un tot *M* a unor obiecte distincte şi bine determinate ***m*** ale gîndirii noastre”.

Însă teoria mulţimilor în forma descrisă de Cantor conducea la *paradoxuri* care provin din „definiţia” foarte permisivă şi vagă a conceptului de mulţime. Însuşi Cantor în 1895 observă că nu se poate vorbi de „mulţimea tuturor ordinalelor” (paradox publicat de Burali-Forti în 1897); mai tîrziu, s-a constatat că există şi alte „mulţimi contradictorii”: „mulţimea tuturor cardinalilor”, „mulţimea tuturor mulţimilor”, „mulţimea mulţimilor care nu se conţin ca element” (paradoxul lui Russel[5]). Prezentăm acest paradox: presupunem că există mulţimea mulţimilor care nu se conţin ca element şi o notăm cu C (în notaţie modernă, $C = \{A \mid A \notin A\}$). Evident, are loc: sau $C \in C$, sau $C \notin C$. Dacă $C \in C$, atunci $C \notin C$ din definiţia lui C, contradicţie. Dacă $C \notin C$, atunci C nu satisface condiţia de definiţie a lui C, deci $C \in C$, contradicţie.

Aceste paradoxuri au putut fi eliminate de *teoria axiomatică a mulţimilor*, care stabileşte *reguli clare de construcţie de mulţimi*. Printre altele, nu se permite considerarea mulţimilor „foarte mari”, care apar mai sus. O primă axiomatizare a fost dată de Zermelo[6] în 1908. Una din axiomele sale (care evită apariţia paradoxurilor de tipul de mai sus) este *Axioma selecţiei*, care în esenţă spune că, dată o „proprietate” [7] *P şi o mulţime A*, există „mulţimea elementelor *din A* care satisfac proprietatea *P*”. Cu alte cuvinte, o proprietate nu determină o *mulţime* (ca în definiţia originală a lui Cantor), ci, *dată o mulţime A*, se poate vorbi doar de existenţa *submulţimii* formată de elementele lui *A* care satisfac *P*.

În 1905 Richard construieşte un paradox de alt tip (simplificat ulterior de Berry şi publicat de Russel în 1906). Să considerăm următorul concept: „cel mai mic număr natural care nu poate fi definit cu mai puţin de 17 cuvinte”. Dacă acest număr ar exista, atunci el *poate fi definit cu 16 cuvinte*, chiar de enunţul anterior (care are 16 cuvinte, număraţi). Contradicţia obţinută arată că nu există un astfel de număr. Pe de altă parte, mulţimea numerelor naturale care pot fi definite cu cel mult 16 cuvinte este finită (căci mulţimea frazelor cu cel mult 16 cuvinte care definesc un număr natural este finită) şi deci *există* numere naturale care nu pot fi definite cu mai puţin de 17 cuvinte. Cel mai mic dintre acestea este un număr… care nu poate exista, conform celor de mai sus!

---

[5] Bertrand Russel (1872-1970), matematician şi filozof britanic.
[6] Ernst Friedrich Ferdinand Zermelo (1871-1953), matematician german.
[7] Mai precis, este vorba de un predicat cu o variabilă liberă.

Paradoxul de mai sus are altă sursă, şi anume *ambiguitatea limbajului* natural, obişnuit. Ce înseamnă exact *a defini* un număr natural?

Din cele spuse reiese că, pe lîngă o axiomatizare a teoriei mulțimilor, trebuie *restrîns limbajul natural* la cîteva modalități bine precizate şi simple de exprimare. În acelaşi timp, posibilitățile trebuie să fie suficient de permisive pentru a putea formula orice enunț matematic. Aceste scopuri sînt realizate de un *limbaj formalizat*.

Vom prezenta intuitiv un astfel de limbaj (o prezentare riguroasă depăşeşte cu mult cadrul şi scopul acestei cărți). Cu această ocazie, vom sublinia anumite aspecte de logică matematică. În continuare vom descrie axiomele teoriei mulțimilor, aplicații (ordinale şi numere naturale). Vom încerca să reliefăm şi modul în care aceste axiome trebuie conştientizate în procesul didactic.

I.1. Limbaj formal, logică

Un minim de cunoştințe privind logica este indispensabil oricărui individ, cu atît mai mult profesorilor de matematică. În manualele de matematică există un capitol dedicat logicii, în clasa a IX-a. Noțiunile şi tehnicile de logică sînt bine alese, în general bine prezentate, şi ar trebui să fie cunoscute de toți elevii şi profesorii. Din păcate, de multe ori acest capitol este privit drept ceva exotic, preferîndu-se o reducere a sa în favoarea unor teme precum funcția de gradul II, lîngă care coexistă – cel puțin temporal. O asemenea alegere facilă este oarecum justificată: e mai uşor de predat o serie de formule şi rețete care solicită mai mult memoria, decît de a încerca o adevărată *formare* a unei gîndiri logice la elevi. Desigur, o astfel de formare nu se realizează doar prin cîteva lecții în clasa a IX-a, ci trebuie văzută ca un obiectiv permanent al lecțiilor de matematică. Existența unor deficiențe în gîndirea logică a elevilor este o chestiune serioasă, care se reflectă nu numai în matematică, ci în orice domeniu: apar dificultăți în înțelegerea legăturilor între diversele noțiuni, se confundă definițiile cu teoremele; în cele din urmă este compromisă însăşi comunicarea coerentă şi înțelegerea informațiilor uzuale.

În teoria axiomatică a mulțimilor (axiomatizarea Zermelo-Fraenkel-Skolem, acceptată în cvasitotalitatea matematicii moderne) *toate obiectele sînt mulțimi*. Altfel spus, *nu se face distincție între conceptele „element" și „mulțime".* Acest punct de vedere este firesc, dacă ne gîndim că o mulțime poate fi element al altei mulțimi; în plus, o teorie axiomatică trebuie să pornească de la un minim de noțiuni primare, iar distincția între element şi mulțime ar complica lucrurile inutil.

Pentru a putea enunța axiomele teoriei mulțimilor, avem nevoie de prezentarea (intuitivă) a limbajului formal al acestei teorii. Subliniem că nu este vorba de o formalizare propriu-zisă. Un limbaj formal prezentat riguros ar ocupa zeci de pagini (un exemplu de formalizare, în cadrul axiomatizării von Neumann-Gödel-Bernays a teoriei mulțimilor, poate fi găsit în REGHIŞ [1981]). Mai întîi descriem *sintaxa limbajului* (regulile după care putem forma expresii corecte ale limbajului formal).

1.1 Definiție. Un *enunț* al limbajului formal (numit şi *expresie* a limbajului formal) este un şir finit de *simboluri*, format după anumite reguli descrise mai jos. Intuitiv, un enunț exprimă un fapt bine determinat despre obiectele la care se referă (în cazul nostru, toate obiectele sînt mulțimi).

Descriem acum tipurile de simboluri şi construcția expresiilor limbajului formal :

i) Există simboluri de tip *nume*, care denumesc *mulțimi* (acestea sînt singurele obiecte pe care le considerăm!). Numele sînt de două feluri: un *nume constant* (pe scurt, *o constantă*) se referă la un obiect bine precizat, iar un *nume variabil* (pe scurt, *o variabilă*) notează un obiect generic (arbitrar, neprecizat). Se presupune că avem la dispoziție o colecție suficient de mare de nume constante şi variabile. Exemple de nume: $x, y, a, b, c, A, B, \ldots$

ii) Simbolurile care notează *relații*: relația de *egalitate*, notată cu simbolul $=$, şi relația de apartenență, notată cu simbolul $\in$. Dacă x, y sînt nume (constante sau variabile), atunci următoarele şiruri de simboluri sînt *expresii* ale limbajului formal:

$x = y$ (citit „x este egal cu y”);

$x \in y$ (citit „x aparține lui y” sau „x este element al lui y”).

iii) Conectorii logici se folosesc pentru a exprima proprietăți mai complexe, pentru a combina mai multe expresii într-una nouă. Conectorii sînt: $\wedge$ (conjuncția, „şi”), $\vee$ (disjuncția, „sau”), $\neg$ (negația, „non”). Dacă E, F sînt expresii (deja construite), atunci sînt expresii şi următoarele şiruri de simboluri:

$E \wedge F$ (citită „E şi F”);

$E \vee F$ (citită „E sau F”);

$\neg E$ (citită „non E”).

iv) Cuantificatorii logici sînt: $\forall$ (cuantificatorul universal, „oricare”), $\exists$ (cuantificatorul existențial, „există”). Cu ajutorul cuantificatorilor (numiți uneori şi *cuantori*) se precizează dacă, într-o expresie, o variabilă se referă la *toate obiectele* sau la *măcar un obiect*. Dacă E este o expresie a limbajului şi x este o variabilă, atunci:

$(\forall x)E$ este expresie (citită „pentru orice x are loc E” sau „pentru orice x, E este adevărată”);

$(\exists x)E$ este expresie (citită „există x astfel încît are loc E” sau „există x astfel încît E este adevărată”).

v) Parantezele rotunde (şi) au rolul de a elimina ambiguitățile. Astfel, în construcțiile precedente, se scrie de exemplu $(E) \wedge (F)$ în loc de $E \wedge F$, sau $(\forall x)(E)$ în loc de $(\forall x)E$ dacă pot

apărea confuzii. Uneori, pentru un plus de claritate, se folosesc şi parantezele pătrate [ ] sau acoladele { }.

Singurele expresii (*enunțuri*) *admise ale limbajului formal sînt cele construite respectînd regulile de mai sus.*

Variabilele unei expresii pot fi *libere* sau *legate*. Spunem că *variabila x este liberă în expresia E* dacă x apare în E, dar E nu conține nici o cuantificare a lui x (adică nici $\forall x$, nici $\exists x$ nu apar în E). Spunem că *variabila x este legată în E* dacă E conține un subşir de simboluri de forma $(\forall x)F$ sau $(\exists x)F$ (unde F este o expresie).

Dacă expresia E conține variabilele *libere* $x_1, \ldots, x_n$, vom sublinia uneori acest lucru scriind $E(x_1, \ldots, x_n)$. Fiind date constantele $c_1, \ldots, c_n$, prin înlocuirea peste tot în E a variabilei x_1 cu c_1, a lui x_2 cu c_2, …, a lui x_n cu c_n se obține o nouă expresie (demonstrați!), notată cu $E(c_1, \ldots, c_n)$. Dacă $x_1, \ldots, x_n$ sînt *toate* variabilele libere din E, atunci $E(c_1, \ldots, c_n)$ este o *propoziție* (adică o expresie care nu are variabile libere). O expresie care are variabile libere se mai numeşte *predicat*.

Vom reveni asupra problemei variabilelor libere sau legate, care are o mare importanță în modul de scriere a enunțurilor matematice.

1.2 Exemple. Presupunem că *x, y, z* sînt variabile şi *a, b* sînt constante. Arătați că următoarele şiruri de simboluri sînt expresii: $x \in y$; $(\forall x)(x \in y)$; $(a \in b) \wedge (x = y)$; $\neg((a \in b) \wedge (x = y))$; $(\forall z)(\exists y)(x \in y)$. Care sînt variabilele libere din fiecare? Şirurile de simboluri: $x(\forall y)$; $x = \ \in$; $\forall y$ nu sînt expresii corecte ale limbajului formal (de ce?).

Să trecem acum la **interpretarea sensului expresiilor** (***semantica limbajului***)**.** Reamintim că o expresie care nu conține variabile libere se numeşte *propoziție*. Oricărei *propoziții* îi asociem o unică *valoare de adevăr*. Valorile de adevăr sînt: 0 (sau *fals*), şi 1 (sau *adevărat*). O propoziție cu valoarea de adevăr 0 se numeşte *propoziție falsă*; o propoziție cu valoarea de adevăr 1 se numeşte *propoziție adevărată*. O propoziție nu poate fi simultan falsă şi adevărată). Descriem acum *regulile* prin care se determină valoarea de adevăr a unei propoziții[8] date.

Fie *a, b* constante şi *x, y* variabile.

i) Propozițiile de forma $a = b$ sînt adevărate exact atunci cînd a şi b denumesc acelaşi obiect.
ii) Valoarea de adevăr a propozițiilor de forma $a \in b$ nu poate fi precizată acum; acest lucru este descris de axiome (în paragraful următor). Evident, intuitiv, $a \in b$ este

[8] Subliniem că doar *propozițiile* au valori de adevăr. Unei expresii cu variabile libere nu i se dă nici o valoare de adevăr.

adevărată dacă şi numai dacă obiectul numit de a este un element al obiectului numit de b.

iii) O propoziţie de forma $E \wedge F$ (unde E şi F sînt propoziţii) este adevărată dacă şi numai dacă E şi F sînt *ambele* adevărate.

iv) O propoziţie de forma $E \vee F$ este adevărată dacă şi numai dacă *măcar una* din propoziţiile E şi F este adevărată (adică sau E, sau F, sau atît E cît şi F sînt adevărate).

v) O propoziţie de forma $\neg E$ este adevărată dacă şi numai dacă propoziţia E este *falsă*.

vi) O propoziţie de forma $(\forall x)E(x)$ (unde variabila x este liberă în E) este adevărată dacă şi numai dacă pentru *orice* obiect c propoziţia $E(c)$ este adevărată.

vii) O propoziţie de forma $(\exists x)E(x)$ (unde variabila x este liberă în E) este adevărată dacă şi numai dacă *există măcar un obiect* c astfel încît propoziţia $E(c)$ să fie adevărată.

1.3 Observaţie. Valoarea de adevăr a propoziţiilor de tipul $E \wedge F$, $E \vee F$, $\neg E$ se poate defini prin *tabele de adevăr*. Iată tabelul de adevăr pentru $E \vee F$, construit după regula iv):

E	F	$E \vee F$
1	1	1
1	0	1
0	1	1
0	0	0

S-au scris pe linii toate combinaţiile posibile de valori de adevăr pentru E şi F. Tabelul se citeşte pe linii: de exemplu, linia 3 a tabelului spune, că, dacă E are valoarea de adevăr 0, iar F are valoarea de adevăr 1, atunci $E \vee F$ are valoarea de adevăr 1.

1.4 Definiţie. a) Două propoziţii E şi F se numesc *echivalente* dacă au aceeaşi valoare de adevăr. Scriem aceasta sub forma $E \equiv F$.

b) Definiţia se poate extinde la expresii oarecare. Două expresii E şi F ce conţin aceleaşi constante şi aceleaşi variabile (fie $x_1, \ldots, x_n$ variabilele din E şi F) sînt numite *echivalente* dacă: orice variabilă care este liberă în E este liberă în F (şi reciproc) şi *propoziţiile* $(\forall x_1)(\forall x_2)\ldots(\forall x_n)E(x_1, \ldots, x_n)$ şi $(\forall x_1)(\forall x_2)\ldots(\forall x_n)F(x_1, \ldots, x_n)$ au aceeaşi valoare de adevăr. Scriem atunci $E \equiv F$, sau $E(x_1, \ldots, x_n) \equiv F(x_1, \ldots, x_n)$ dacă vrem să evidenţiem variabilele libere.

1.5 Exerciţiu. Dacă E, F şi G sînt expresii, avem echivalenţele :

$\neg(E \wedge F) \equiv (\neg E) \vee (\neg F)$; $\neg(E \vee F) \equiv (\neg E) \wedge (\neg F)$; (legile lui DeMorgan)

$(E \wedge F) \vee G \equiv (E \vee G) \wedge (F \vee G)$; (distributivitatea lui $\vee$ faţă de $\wedge$)

$(E \vee F) \wedge G \equiv (E \wedge G) \vee (F \wedge G)$; (distributivitatea lui $\wedge$ faţă de $\vee$)

$\neg((\forall x)E) \equiv (\exists x)(\neg E)$; $\neg((\exists x)E) \equiv (\forall x)(\neg E)$ (legile de negare a cuantificatorilor).

De exemplu, $\neg(E \wedge F) \equiv (\neg E) \vee (\neg F)$ se poate demonstra cu următorul tabel de adevăr:

E	F	$E \wedge F$	$\neg(E \wedge F)$	$\neg E$	$\neg F$	$(\neg E) \vee (\neg F)$
1	1	1	0	0	0	0
1	0	0	1	0	1	1
0	1	0	1	1	0	1
0	0	0	1	1	1	1

Identitatea coloanelor $\neg(E \wedge F)$ şi $(\neg E) \vee (\neg F)$ demonstrează echivalenţa cerută.

Legile lui DeMorgan arată că am fi putut reduce setul de conectori logici şi cuantificatori, de exemplu la $\forall$, $\neg$, $\wedge$.

Introducem următoarele *prescurtări* uzuale. Fie E, F expresii. Atunci scriem:

$E \rightarrow F$ în loc de $(\neg E) \vee F$ şi citim „E implică F" sau „dacă E, atunci F";

$E \leftrightarrow F$ în loc de $(E \rightarrow F) \wedge (E \rightarrow F)$ şi citim „E este echivalent cu F".

1.6 Exerciţiu. Scrieţi tabelele de adevăr pentru conectorii $\rightarrow$ şi $\leftrightarrow$. Demonstraţi că, dacă E şi F sînt propoziţii, $E \leftrightarrow F$ este adevărată dacă şi numai dacă E şi F au aceeaşi valoare de adevăr.

Insistăm asupra *implicaţiei*, $\rightarrow$. Se justifică intuitiv că $E \rightarrow F$ este acelaşi lucru cu $(\neg E) \vee F$, astfel: "$E \rightarrow F$" înseamnă "dacă E este adevărată, atunci F este adevărată". Altfel spus, sau E este falsă (adică are loc $\neg E$), sau E este adevărată şi atunci automat F este adevărată (adică are loc F); pe scurt, $(\neg E) \vee F$. Este important de conştientizat această echivalenţă logică, utilă mai ales cînd trebuie negată o implicaţie (lucru care intervine frecvent, de exemplu în cazul demonstraţiilor prin reducere la absurd). Astfel, faptul că $E \rightarrow F$ este falsă înseamnă că are loc $(E \rightarrow F) \equiv \neg(\neg E) \vee F) \equiv E \wedge (\neg F)$ (ipoteza este adevărată şi totuşi concluzia este falsă). Această interpretare este conformă cu intuiţia („bunul-simţ"). De altfel, concluziile bazate pe un calcul logic formal trebuie totdeauna interpretate intuitiv, proces absolut necesar în înţelegerea unor demonstraţii (sau în găsirea unor soluţii la o problemă dată).

Vom mai folosi şi alte prescurtări, larg utilizate, de exemplu $x \neq y$ pentru $\neg\, (x = y)$ sau $x \notin y$ în loc de $\neg\, (x \in y)$.

Dacă propoziţia $E \rightarrow F$ este adevărată, scriem atunci $E \Rightarrow F$. Analog, scrierea $E \Leftrightarrow F$ înseamnă că propoziţia $E \leftrightarrow F$ este adevărată.

1.7 Observaţie. Orice teoremă matematică (propoziţie, lemă etc.) poate fi scrisă în limbaj formal. Expresia obţinută trebuie să fie din punct de vedere logic o *propoziţie* (*nu trebuie să aibă variabile libere*). De exemplu, teorema împărţirii cu rest în $\mathbb{N}$ se poate scrie formal:

$(\forall a)(\forall b)[(a \in \mathbb{N} \wedge b \in \mathbb{N} \wedge b \neq 0) \Rightarrow (\exists q)(\exists r)(q \in \mathbb{N} \wedge r \in \mathbb{N} \wedge a = bq + r \wedge r < b)]$.

I.2. Axiomatica mulțimilor

Prezentăm cîteva elemente din teoria axiomatică Zermelo-Fraenkel-Skolem (ZFS) a mulțimilor. Pentru o tratare mai detaliată, incluzînd multe teme interesante (ordinali, cardinali, axioma alegerii etc.), vezi SCORPAN [1996].

Nu putem *defini* un obiect fără a face referire la alte obiecte, presupuse cunoscute. Aceste obiecte "cunoscute" trebuie la rîndul lor definite… Se vede că acest proces nu poate continua la infinit.

Aşadar, trebuie să considerăm în cele din urmă *noțiuni care nu se definesc* (*noțiuni primare*); cu ajutorul lor vom putea defini alte obiecte. Aceasta este un principiu de bază în orice teorie axiomatică.

În axiomatizarea teoriei mulțimilor, noțiunile de *mulțime* şi de *relație de apartenență* se consideră *noțiuni primare* (nu se definesc) şi *toate obiectele teoriei sînt mulțimi* (în particular, toate elementele unei mulțimi sînt tot mulțimi!). Aceste noțiuni satisfac un set de *axiome* (care, într-un anumit sens, *definesc* obiectele respective). Altfel spus, nu ne interesază *ce sînt* mulțimile, ci *cum se comportă* unele față de altele şi față de relația de apartenență. Axiomele stabilesc regulile care se aplică obiectelor abstracte numite mulțimi şi relației de apartenență.

Axiomele nu sînt decît *propoziții* (din limbajul formal construit anterior) care sînt *declarate şi acceptate ca adevărate.* Orice altă afirmație despre mulțimi trebuie *demonstrată* pornind de la axiome. În acest mod se deduc toate proprietățile „uzuale” ale teoriei mulțimilor.

Deşi, după cum am spus, în teoria axiomatică *elementele unei mulțimi sînt tot mulțimi*, vom adopta (pe cît posibil), pentru a nu crea confuzii cititorului, distincția tradițională în notație: în general, se notează *mulțimile cu majuscule* ($A, B, \ldots$), iar *elementele mulțimilor cu minuscule* ($a, b, \ldots$). Dacă A este o mulțime şi a este un element al lui A, atunci scriem $a \in A$ (citit *„a aparține lui A”* sau *„A conține pe a”*). Dacă a nu este element al mulțimii A, scriem $a \notin A$.

2.1 Axioma extensionalității: *Pentru orice două mulțimi A şi B, avem :*

$$[(\forall a)\ (a \in A \leftrightarrow a \in B)] \to A = B.$$

Mai riguros spus, propoziția următoare este adevărată:

$$(\forall A)\ (\forall B)\ \{[(\forall a)\ (a \in A \leftrightarrow a \in B)] \to A = B\}.$$

Această axiomă nu spune decît că *o mulțime este determinată de elementele sale*. Cu alte cuvinte, *dacă două mulțimi au aceleaşi elemente, atunci mulțimile coincid*.

Observăm că are loc şi implicația inversă: dacă $A = B$, atunci orice element a care aparține lui A aparține şi lui B. Acest fapt este evident: A şi B denumesc acelaşi obiect, deci orice enunț referitor la A este adevărat şi pentru B (şi reciproc).

Dacă A şi B sînt două mulțimi, vom scrie $A \subseteq B$ (şi citim *A inclus în B* sau *A este submulțime a lui B*) dacă orice element al lui A aparține şi lui B: $(\forall a)\ [(a \in A) \to (a \in B)]$. În caz contrar, notăm $A \not\subset B$.

Cu această notație, avem: $(\forall A)\ (\forall B)\ [\ (A = B) \leftrightarrow\ (A \subseteq B \wedge B \subseteq A)]$.

Pe această proprietate se bazează majoritatea demonstrațiilor de egalitate de mulțimi: pentru a demonstra că $A = B$, arătăm că orice element al lui A aparține şi lui B (adică $A \subseteq B$) şi reciproc ($B \subseteq A$).

Axiomele care urmează sînt toate de următorul tip: *fiind date una sau mai multe mulțimi, se garantează existența unei noi mulțimi cu anumite proprietăți* (construită cu ajutorul mulțimilor inițiale). Cu alte cuvinte, axiomele descriu *construcții permise în cadrul teoriei*. Se regăseşte astfel motivul pentru care a fost construită teoria: evitarea paradoxurilor generate de construcții de mulțimi „prea mari”.

2.2 Axioma mulțimii părților unei mulțimi. $(\forall M)\ (\exists P)\ ((\forall A)(A \in P \leftrightarrow A \subseteq M))$.

În cuvinte: fiind dată o mulțime M, există o mulțime P astfel încît elementele lui P sînt exact submulțimile lui M.

Mulțimea P a cărei existență este postulată mai sus este unic determinată de mulțimea M. Într-adevăr, dacă şi Q satisface condiția $(\forall A\ (A \in Q \leftrightarrow A \subseteq M))$, atunci avem, pentru orice mulțime A: $A \in Q \leftrightarrow A \subseteq M \leftrightarrow A \in P$. Din axioma extensionalității obținem că $P = Q$.

Notația tradițională pentru P este $\mathcal{P}(M)$ (mulțimea părților lui M).

2.3 Axioma reuniunii. *Pentru orice mulțime A* (*subînțeles: avînd ca elemente tot mulțimi*), *se admite existența unei mulțimi ale cărei elemente sînt elementele mulțimilor din A*, *adică*:

$$(\forall A)\ (\exists U)\ (\forall x)\ [(x \in U) \leftrightarrow (\exists a)\ (a \in A \wedge x \in a)].$$

Pentru înțelegerea acestei axiome, este util să privim A ca pe o *familie de mulțimi*. Axioma de mai sus nu face decît să postuleze existența *reuniunii* acestei familii de mulțimi.

Mulțimea U – a cărei existență este garantată de axiomă – este unic determinată de A (demonstrați!) şi se notează $\bigcup A$ sau $\bigcup_{x \in A} x$ sau $\bigcup\{x \mid x \in A\}$. A se remarca în acest context futilitatea distincției dintre element şi mulțime.

2.4 Axioma-schemă a substituției

Nu este vorba de o simplă axiomă, ci de o *schemă* de axiome. Mai precis, pentru orice expresie (de un anumit tip) a limbajului formal se obține o axiomă. Aşadar, avem de a face cu o infinitate de axiome.

Pentru enunț, avem nevoie de o **definiție**. O expresie $E(x, y)$ cu exact două variabile libere x şi y se numeşte *relație funcțională* dacă pentru orice x există cel mult un y astfel încît $E(x, y)$ să fie adevărată:

$$(\forall x)(\forall y)(\forall z)\ ((E(x, y) \wedge E(x, z)) \to y = z).$$

Intuitiv, putem privi o relație funcțională ca pe o „funcție parțial definită”: pentru anumiți x există un unic y astfel încît $E(x, y)$ să aibă loc; se notează uneori chiar „funcțional”, $y = \widetilde{E}(x)$ în loc de $E(x, y)$. Observăm că nu este neapărat adevărat că $(\forall x)(\exists y)E(x, y)$.

În termeni mai puțin formali, axioma-schemă a substituției afirmă că: *Pentru orice relație funcțională $E(x, y)$ şi pentru orice mulțime a, există „imaginea prin E a mulțimii a”.*

Evident, trebuie să definim formal conceptul de „imagine a unei mulțimi printr-o relație funcțională”. Spunem că mulțimea b este *imaginea mulțimii a prin relația funcțională* $E(x, y)$ dacă „elementele lui b sînt de forma $\widetilde{E}(x)$, cu $x \in a$”, adică:

$$(\forall y)[y \in b \leftrightarrow (\exists x)(x \in a \wedge E(x, y))].$$

Axioma-schemă a substituției este: *pentru orice relație funcțională $E(x, y)$, are loc:*

$$(\forall a)(\exists b)(\forall y)[y \in b \leftrightarrow (\exists x)(x \in a \wedge E(x, y))].$$

Subliniem din nou că *se obține cîte o axiomă pentru fiecare alegere a unei relații funcționale E*. Nu se pot condensa toate aceste enunțuri într-unul singur, de tipul

$$(\forall E \text{ relație funcțională})(\forall a)(\exists b)(\forall y)[y \in b \leftrightarrow (\exists x)(x \in a \wedge E(x, y))],$$

deoarece acesta *nu* este o expresie a limbajului formal: E nu denumeşte un *obiect* legitim (o mulțime), ci o *expresie*.

Folosind axioma extensionalității, se demonstrează imediat că *imaginea unei mulțimi printr-o relație funcțională este unic determinată* (mulțimea b a cărei existență este postulată de axioma schemă a substituției este unic determinată de E şi b).

2.5 Consecință (***Schema de comprehensiune***). *Pentru orice mulțime A şi pentru orice expresie cu o variabilă liberă $P(x)$, există submulțimea elementelor din A pentru care P este adevărată. Formal,* $(\forall A)(\exists B)(\forall x)[x \in B \leftrightarrow (x \in A \wedge P(x))]$.[9]

Demonstrație. Fie expresia $E(x,y)$: "$(x = y) \wedge P(y)$". Afirmăm că E este o relație funcțională. Într-adevăr, fie x, y, z cu $E(x,y)$ şi $E(x,z)$ adevărate. Atunci $x = y$ şi $x = z$, deci $y = z$.

Conform axiomei substituției, pentru mulțimea A există o mulțime B astfel încît:

$$(\forall y)[y \in B \leftrightarrow (\exists x)(x \in A \wedge E(x, y))],$$

adică $y \in B \leftrightarrow (\exists x)(x \in A \wedge (x = y) \wedge P(y))$, ceea ce revine la a spune că $y \in B \leftrightarrow (y \in A \wedge P(y))$, ceea ce trebuia demonstrat. □

Iarăşi, axioma extensionalității asigură că A şi $P(x)$ determină *unic* mulțimea B din enunț. Această mulțime se notează tradițional:

$\{x \in A \mid P(x)\}$ (citit „mulțimea elementelor din A care satisfac P”).

2.6 Observație. Dacă se presupune că există măcar o mulțime[10] A, rezultatul de mai sus asigură existența unei (unice) mulțimi ce nu conține nici un element, numită *mulțimea vidă* şi

[9] În axiomatizarea lui Zermelo din 1908, acest rezultat era enunțat ca axiomă şi era numit *Axioma selecției*.

notată cu $\varnothing$.[11] Într-adevăr, fie $P(x)$: "$x \neq x$". Din schema de comprehensiune, există $\varnothing := \{x \in A \mid x \neq x\}$. Pentru orice x, avem $x \notin \varnothing$ (dacă $x \in \varnothing$, atunci $x \neq x$, absurd). Unicitatea lui $\varnothing$ este o consecință a axiomei extensionalității. Notăm deci $\varnothing := \{x \in A \mid x \neq x\}$.

Pentru orice mulțime M are loc $\varnothing \subseteq M$. Este instructiv să prezentăm în detaliu acest argument. Conform definiției, avem $\varnothing \subseteq M$ dacă şi numai dacă $\forall x\ (x \in \varnothing \to x \in M)$. Dar expresia $x \in \varnothing \to x \in M$ este, conform definiției, o prescurtare pentru $\neg(x \in \varnothing) \vee (x \in M)$, care este adevărată, căci $\neg(x \in \varnothing)$ este adevărată.

Termenul de *comprehensiune* descrie modalitatea de a preciza o mulțime prin enunțarea unei proprietăți pe care o au doar elementele mulțimii şi numai ele. S-a văzut că acest concept, care a stat la baza teoriei naive a mulțimilor, duce la paradoxuri; schema de comprehensiune restrînge această modalitate doar la posibilitatea următoare: pentru orice *mulțime dată M* şi orice „proprietate” P, există *submulțimea* elementelor lui M care satisfac P.

Cealaltă modalitate de a da o mulțime este prin *extensiune*, adică prin enumerarea tuturor elementelor sale. Astfel, fiind date elementele distincte $x_1, \ldots, x_n$, există mulțimea X ale cărei elemente sînt exact $x_1, \ldots, x_n$. Acest lucru este asigurat de schema de comprehensiune; scrierea $X = \{x_1, \ldots, x_n\}$ este o prescurtare a scrierii $(\forall x)(x \in X \leftrightarrow (x = x_1 \vee x = x_2 \vee \ldots \vee x = x_n))$.

2.7 Observație. Putem acum defini şi alte „operații cu mulțimi”. Astfel, pentru orice două mulțimi A şi B, arătați că există mulțimile:

$\{x \in A \mid x \in B\}$ (notată $A \cap B$ şi numită *intersecția* lui A şi B)

$\{x \in A \mid x \notin B\}$ (notată $A \setminus B$ şi numită *diferența* lui A şi B).

Demonstrați că $A \cap B = B \cap A$.

I.3. Clase, relații, funcții

Nu există o „mulțime a tuturor mulțimilor”, căci acest concept conduce la paradoxuri. Dacă ar exista mulțimea tuturor mulțimilor, fie aceasta $\boldsymbol{A}$, atunci, conform schemei de comprehensiune, ar exista şi mulțimea $C = \{B \in \boldsymbol{A} \mid B \notin B\}$. Se vede că regăsim paradoxul lui Russel. Astfel de colecții „foarte mari” de obiecte apar însă frecvent în matematică (dorim de exemplu să vorbim de o proprietate pe care o au „toate” grupurile) şi este necesară precizarea unui cadru riguros pentru aceste situații. O rezolvare rezonabilă este dată de conceptul de *clasă*.

---

[10] Acest fapt este postulat de axioma infinității, enunțată mai jos.

[11] Nu este litera grecească majusculă *phi*, Φ, ci un simbol matematic derivat dintr-o literă norvegiană, Ø.

În cadrul teoriei Gödel-Bernays (GB), *clasa* este o noțiune primară (nu se definește clasa, ci este dat un set de axiome referitoare la clase; mulțimile vor fi un tip particular de clase – cele care sînt elemente ale altor clase). Teoria astfel dezvoltată este însă considerabil mai complicată decît ZFS [12].

În teoria ZFS, prin *clasă* se înțelege o expresie cu o variabilă liberă (un predicat cu o variabilă)[13]. Cu alte cuvinte, o proprietate nu mai definește o *mulțime* de obiecte, ci este privită ea însăși ca o entitate și o numim *clasă*. O clasă *nu* este însă un obiect al teoriei ZFS, ci este o expresie a limbajului formal (cf. comentariul de la axioma-schemă a substituției). De exemplu, predicatul $P(x)$: „$x = x$" este evident satisfăcut de orice mulțime x; acest predicat definește „clasa tuturor mulțimilor". Abuzînd de limbajul de la mulțimi, fiind dată o clasă $P(x)$, în loc să se spună ca un anumit x satisface P sau „$P(x)$ este adevărată", se spune „x aparține clasei P" sau „x este un element al clasei P".

Observăm că orice mulțime a definește o clasă, anume „$x \in a$".

Reciproc, spunem că o clasă $P(x)$ *corespunde* unei mulțimi M dacă are loc $\forall x\ (P(x) \leftrightarrow x \in M)$: obiectele care satisfac P sînt exact elementele lui M. Uneori spunem în acest caz chiar că P *este* o mulțime.

În acest sens, *clasa tuturor mulțimilor nu corespunde unei mulțimi*. Demonstrația a fost dată chiar la începutul acestui paragraf!

Se pot defini și *operații cu clase*, prin analogie cu cele de la mulțimi. Astfel, dacă $P(x)$ și $Q(x)$ sînt clase, definim *reuniunea* claselor P și Q ca fiind clasa $P(x) \vee Q(x)$; *intersecția* lor este clasa $P(x) \wedge Q(x)$. Cum s-ar defini *diferența* lor? Dar faptul că clasa P este *inclusă* în clasa Q?

În această terminologie, schema de comprehensiune nu spune altceva decît că *intersecția dintre o clasă și o mulțime este o mulțime.*

Apare acum destul de clar că exprimări de genul „mulțimea tuturor grupurilor" nu sînt legitime, o exprimare corectă fiind „clasa tuturor grupurilor". Noțiunea de clasă este esențială în *teoria categoriilor*.

Să trecem la un alt concept fundamental, anume la cel de *funcție*. Pentru aceasta, avem nevoie de noțiunea de *cuplu* (*pereche ordonată*). Începem cu un rezultat interesant și prin sine.

3.1 Propoziție ***(Teorema perechii)****. Fie a și b două mulțimi. Atunci există o mulțime c care are ca elemente pe a și pe b și numai pe ele. Formal:*

$$(\forall a)(\forall b)(\exists c)(\forall x)\ [(x \in c) \leftrightarrow (x = a \vee x = b)]$$

Mulțimea c de mai sus este unic determinată de a și b și se notează $\{a, b\}$.

---

[12] În plus, s-a arătat că orice enunț despre mulțimi demonstrabil în GB este demonstrabil în ZFS.
[13] Această interpretare pentru clase a fost prezentată de W. Quine în 1963.

Demonstrație. Ideea este de a construi o mulțime cu două elemente D şi de a obține $\{a, b\}$ ca imaginea lui D printr-o relație funcțională bine aleasă (se aplică deci axioma substituției).

Ştim că există mulțimea vidă $\varnothing$. Construim (cu axioma mulțimii părților) mulțimea $\mathcal{P}(\varnothing)$, care are un element (avem $\varnothing \subseteq \varnothing$, deci $\varnothing \in \mathcal{P}(\varnothing)$; $\varnothing$ este chiar unicul element al lui $\mathcal{P}(\varnothing)$, deci $\mathcal{P}(\varnothing) = \{\varnothing\}$). Cum $\varnothing$ nu are nici un element, deducem că $\mathcal{P}(\varnothing) \neq \varnothing$. Construim acum $\mathcal{P}(\mathcal{P}(\varnothing)) = \mathcal{P}(\{\varnothing\})$. Unicele mulțimi incluse în $\{\varnothing\}$ sînt $\varnothing$ şi $\{\varnothing\}$, deci $\mathcal{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$ are două elemente (cum am dorit).

Fie $E(x, y)$: "$(x = \varnothing \wedge y = a) \vee (x = \{\varnothing\} \wedge y = b)$" (verificați că este o relație funcțională) Imaginea prin E a lui $\mathcal{P}(\{\varnothing\})$ este chiar mulțimea căutată c.

Unicitatea lui c rezultă din axioma extensionalității. □

3.2 Exercițiu. Fie a şi b mulțimi. Demonstrați că există reuniunea lor $a \bigcup b$ (adică unica mulțime cu proprietatea $\forall x[(x \in a \bigcup b) \leftrightarrow (x \in a \vee x \in b)]$).

Intuitiv, noțiunea de *cuplu* (*pereche ordonată*) format de elementele a şi b diferă de $\{a, b\}$, prin faptul că avem o „ordine": a este primul, iar b este al doilea. Această distincție între a şi b se realizează prin:

3.3 Definiție. Fie a şi b mulțimi. Aplicînd propoziția de mai sus mulțimilor a şi a, există mulțimea $\{a\}$; există şi $\{a, b\}$. Aplicînd din nou propoziția, există mulțimea $\{\{a\}, \{a, b\}\}$, care se notează cu (a, b) şi se numeşte *perechea ordonată* (*cuplul*) format de a şi b. Observați că, dacă $a = b$, atunci $(a, b) = \{\{a\}\}$.

Această idee de introducere a noțiunii de cuplu este atribuită lui Kuratowski. Are loc proprietatea fundamentală următoare (demonstrați!):

3.4 Propoziție. *Fie a, b, a', b' mulțimi. Atunci are loc:* $(a, b) = (a', b') \leftrightarrow a = a'$ *şi* $b = b'$. □

Astfel, spre deosebire de *mulțimea* $\{a, b\}$, în *cuplul* (a, b) *contează ordinea* elementelor a şi b; dacă $a \neq b$, atunci $(a, b) \neq (b, a)$, însă $\{a, b\} = \{b, a\}$.

Avînd definită noțiunea de cuplu, definim noțiunea de *triplet*:

$$(a, b, c) := ((a, b), c)$$

şi, prin recurență, *n-uplu*, $\forall n \geq 3$ (pentru o tratare riguroasă a inducției şi recurenței, vezi I.4.20)

$$(a_1, \ldots, a_n) := ((a_1, \ldots, a_{n-1}), a_n).$$

Are loc: $(a_1, \ldots, a_n) = (b_1, \ldots, b_n) \leftrightarrow a_1 = b_1 \wedge \ldots \wedge a_n = b_n$.

În manualele de liceu (şi în multe alte cărți de matematică), o *funcție* definită pe o mulțime A cu valori într-o mulțime B este „definită" (mai bine spus descrisă) ca fiind „*un procedeu (lege), prin care oricărui element din A i se asociază un unic element din B*". Intuitiv, descrierea este corectă (dar vagă, deoarece foloseşte noțiunea nedefinită de *procedeu* (*lege*)); în plus, se subînțelege că pentru orice funcție se poate descrie un *procedeu* (*algoritm*) de

obținere a imaginii oricărui element prin funcția dată. Acest lucru nu este necesar şi în matematică se întîlnesc exemple de funcții pentru care acest fapt nu are loc.

Se observă însă că o funcție $f : A \to B$ este perfect determinată de *graficul* său, adică de mulțimea cuplurilor $\{(a, f(a)) \mid a \in A\}$. Aceasta este şi ideea definiției conceptului de funcție în cadrul unei tratări riguroase. Începem cu alte două noțiuni, şi ele fundamentale:

3.5 Definiție. Fie A şi B mulțimi. Numim *produsul cartezian*[14] al mulțimilor A şi B mulțimea $A \times B := \{(a, b) \mid a \in A \wedge b \in B\}$.

Avem dreptul de a defini o astfel de mulțime? Ar trebui să arătăm că ne încadrăm în schema de comprehensiune, adică să indicăm o mulțime a cărei existență este certă, care să conțină toate perechile de forma (a, b) cu $a \in A$ şi $b \in B$. Dar $(a, b) = \{\{a\}, \{a, b\}\}$. Observăm că avem $\{a\} \in \mathcal{P}(A \cup B)$ şi $\{a, b\} \in \mathcal{P}(A \cup B)$, deci $\{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$. Astfel, putem defini, respectînd schema de comprehensiune:

$$A \times B := \{c \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid (\exists a)(\exists b)[c = (a, b) \wedge a \in A \wedge b \in B]\}.$$

Folosind produsul cartezian putem defini noțiunile de *relație* şi de *funcție*:

3.6 Definiție. Fie A şi B două mulțimi.

a) Numim *relație binară între A şi B* (sau *de la A la B*) orice triplet de forma (A, B, ρ), unde $\rho \subseteq A \times B$. Uneori vom exprima acest fapt sub forma „ρ este o relație între A şi B”. Dacă $A = B$, scriem (A, ρ) şi spunem că ρ este *o relație pe A*. Adeseori, în loc de $(x, y) \in \rho$ se scrie $x\rho y$. Dacă sînt subînțelese mulțimile A şi B, se spune, simplu, relația ρ în loc de (A, B, ρ).

b) O relație binară f de la A la B se numeşte *funcție* (sau *aplicație*) *definită pe A cu valori în B* dacă pentru orice $a \in A$ există *un unic* $b \in B$ astfel încît $(a, b) \in f$. Formal, tripletul (A, b, f) este funcție de la A la B dacă:

$$\begin{gathered}(f \subseteq A \times B) \wedge (\forall a)\{(a \in A) \to (\exists b)[(b \in B) \wedge (a, b) \in f]\} \wedge \\ (\forall a)(\forall b)(\forall b')\{(a \in A) \wedge (b \in B) \wedge (b' \in B) \wedge (a, b) \in f \wedge (a, b') \in f \to (b = b')\}\end{gathered} \qquad (*)$$

Întrucît pentru orice $a \in A$ există *un unic* $b \in B$ astfel încît $(a, b) \in f$, se scrie:

„$f(a) = b$” în loc de „$(a, b) \in f$”.

Se mai spune „*f este o funcție* (*aplicație*) *de la A la B*” şi se notează aceasta prin $f : A \to B$ sau $A \xrightarrow{f} B$. *Notația* $f : A \to B$ *nu este decît o prescurtare a expresiei* (*).

Mulțimea A se numeşte *domeniul* funcției f şi B se numeşte *codomeniul* lui f. Orice element a din domeniul lui f se numeşte *argument* al funcției f. Dacă $a \in A$ şi $b \in B$ astfel încît $f(a) = b$, b se numeşte *valoarea funcției f în a*.

Pentru orice mulțime A, notăm cu $\mathbf{1}_A$ sau cu id_A *funcția identitate* a mulțimii A, anume: $id_A(a) = a$, $\forall a \in A$.

[14] În onoarea lui René Descartes (1596-1650), al cărui nume latinizat era Cartesius.

Dacă adoptăm punctul de vedere naiv: o funcție $f : A \to B$ este o „lege de corespondență” prin care oricărui element a din A i se asociază un unic element $f(a)$ din B, atunci mulțimea $\{(a, f(a)) \mid a \in A\} \subseteq A \times B$ se numeşte *graficul* lui f. Astfel, definiția **3.6.**b) identifică o funcție cu graficul ei.

3.7 Observație. Condiția (*) se scrie, mai puțin formalizat:

$$(f \subseteq A \times B) \text{ şi } \forall a \in A, \exists\, b \in B \text{ astfel încît } (a, b) \in f \text{ şi}$$

$$\forall a \in A, \forall b, b' \in B, (a, b) \in f \text{ şi } (a, b') \in f \text{ implică } b = b'.$$

Observăm că, în expresii, şirurile de forma "$(\forall a)(a \in A)$" se scriu adesea prescurtat "$\forall a \in A$". Această convenție, larg răspîndită, ascunde o capcană: o implicație, de genul $(\forall a)[(a \in A) \to P(a)]$, se scrie adesea "$\forall a \in A, P(a)$", în care implicația $\to$ nu apare explicit. Trebuie conştientizat acest fapt, mai ales cînd apare necesitatea negării unei astfel de expresii: negația ei este $(\exists a)\{(a \in A) \wedge \neg P(a)\}$, lucru care nu este clar din scrierea prescurtată (dar este destul de clar din punct de vedere intuitiv).

3.8 Observație. O expresie cu exact două variabile libere se numeşte *relație*. Pentru orice relație $R(x, y)$ putem defini "*domeniul*" D_R şi "*imaginea*" I_R ca fiind *clasele*:

$$D_R(x): \text{"}(\exists y)R(x, y)\text{"}$$

$$I_R(y): \text{"}(\exists x)R(x, y)\text{"}$$

Demonstrați că, dacă clasele D_R şi I_R sînt mulțimi, atunci relației $R(x, y)$ i se asociază o relație ρ între D_R şi I_R (în sensul definiției **3.6.**a), $\rho := \{(x, y) \in D_R \times I_R \mid R(x, y) \text{ adevărată}\}$. Mai mult, această relație este *funcție* (în sensul definiției **3.6.**b) dacă şi numai dacă R este *relație funcțională*. Invers, unei funcții $f : A \to B$ i se asociază o relație funcțională $F(x, y)$: "$x \in A \wedge y = f(x)$".

Demonstrați că, dacă R este relație funcțională şi D_R este mulțime, atunci I_R este mulțime. Reciproca este adevărată?

3.9 Exercițiu. Fie A o mulțime. Cîte funcții $\varphi : \varnothing \to A$ (respectiv $\varphi : A \to \varnothing$) există?

3.10 Definiție. Fie $f : A \to B$ o funcție. Dacă $A' \subseteq A$, se defineşte *imaginea lui A' prin f* ca fiind imaginea mulțimii A' prin relația funcțională asociată lui f. Cu alte cuvinte, definim

$$f[A'] = \{y \in B \mid (\exists x)(x \in A' \wedge f(x) = y)\}$$

Notația tradițională pentru imaginea lui A' prin f este $f(A')$; nu se poate folosi o astfel de notație în teoria axiomatică a mulțimilor, pentru că A' poate fi simultan submulțime a lui A şi element al lui A (puteți da exemplu de un astfel de caz?) şi este foarte posibil ca $f(A')$ (valoarea în A' a lui f) să difere de $f[A']$ (imaginea submulțimii A' prin f).

3.11 Definiție. Fie I o mulțime (interpretată ca mulțime de „indici”). O funcție $b : I \to M$, unde M este o mulțime, se numeşte *familie de mulțimi indexată după I*. Notații tradiționale pentru această noțiune: $(B_i)_{i \in I}$ (unde $B_i := b(i)$), sau $\{B_i \mid i \in I\}$.

Dacă $(B_i)_{i \in I}$ este o familie de mulțimi ca mai sus, *reuniunea familiei* $\{B_i\}_{i\in I}$ este reuniunea imaginii funcției b:

$$\bigcup A = \bigcup_{i\in I} B_i := \{x \in M \mid \exists i \in I \text{ astfel încît } x \in B_i\}.$$

Intersecția familiei $\{B_i\}_{i\in I}$ este, prin definiție

$$\bigcap_{i\in I} B_i := \{x \mid \forall i \in I, x \in B_i\}.$$

De exemplu, dacă $I = \{1, 2\}$ şi $\{B_i\}_{i\in I} = \{B_1, B_2\}$,

$$\bigcup\{B_1, B_2\} = \bigcup_{i\in I} B_i = B_1\bigcup B_2; \text{ la fel, } \bigcap\{B_1, B_2\} = \bigcap_{i\in I} B_i = B_1\bigcap B_2.$$

Se spune că *reuniunea familiei* $\{B_i\}_{i\in I}$ *este disjunctă* dacă $\{B_i\}_{i\in I}$ sînt disjuncte două cîte două: $B_i\bigcap B_j = \varnothing$ dacă $i \neq j$.

3.12 Propoziție. *Pentru orice mulțimi A, B, C, au loc egalitățile:*

i) $\varnothing\bigcap A = \varnothing$, $\varnothing\bigcup A = A$, $A \setminus \varnothing = A$, $A \setminus A = \varnothing$;

ii) $A\bigcap B \subseteq A$, $A\bigcap B \subseteq B$, $A \subseteq A\bigcup B$, $B \subseteq A\bigcup B$;

iii) $A\bigcap B = B\bigcap A$, $A\bigcup B = B\bigcup A$;

iv) $A\bigcap(B\bigcap C) = (A\bigcap B)\bigcap C$, $A\bigcup(B\bigcup C) = (A\bigcup B)\bigcup C$;

v) $A\bigcap(B\bigcup C) = (A\bigcap B)\bigcup(A\bigcap C)$, $A\bigcup(B\bigcap C) = (A\bigcup B)\bigcap(A\bigcup C)$;

vi) $A\bigcup A = A = A\bigcap A$. □

3.13 Definiție. Se numeşte *inversă a unei relații* (A, B, ρ) relația (B, A, ρ^{-1}) unde $\rho^{-1} = \{(b, a) \mid (a, b) \in \rho\} \subseteq B \times A$.

Fie relațiile (A, B, ρ) şi (B, C, τ). Relația $(A, C, \tau\circ\rho)$, unde

$$\tau\circ\rho = \{(a, c) \in A \times C \mid (\exists b)(b \in B \wedge a\rho b \wedge b\tau c)\}$$

este numită *compusa* (sau *compunerea*) *relațiilor* τ şi ρ.

3.14 Propoziție. *a) Fiind date funcțiile* $u : A \to B$, $v : B \to C$, *compusa* $v\circ u$ *este tot o funcție,* $v\circ u : A \to C$, *şi,* $\forall a \in A$, *are loc:*

$$(v\circ u)(a) = v(u(a)).$$

b) Pentru orice relații (A, B, ρ), (B, C, τ), (C, D, η), *avem* $(\eta\circ\tau)\circ\rho = \eta\circ(\tau\circ\rho)$ (*compunerea relațiilor este asociativă*). *În particular, compunerea funcțiilor este asociativă.* □

Se disting următoarele tipuri remarcabile de funcții:

3.15 Definiție. Fie $f : A \to B$ o funcție. Spunem că f este:

i) *funcție injectivă* dacă $\forall x, y \in A, f(x) = f(y) \Rightarrow x = y$;

ii) *funcție surjectivă* dacă $\forall y \in B$, $\exists\, x \in A$ astfel încît $f(x) = y$;

iii) *funcție bijectivă* dacă este injectivă şi surjectivă;

iv) *funcție inversabilă* dacă $\exists\ g : B \to A$ (numită inversa lui f) astfel încît $(g\circ f)(x) = x$, $\forall x \in A$ şi $(f\circ g)(y) = y$, $\forall y \in B$.

Notînd, pentru o mulțime M, prin $\mathbf{1}_M : M \to M$ funcția $\mathbf{1}_M(x) = x$, $\forall x \in M$ (numită şi *funcția identitate* a lui M, notată şi cu id_M sau id), condițiile ce definesc funcțiile inversabile pot fi rescrise în modul următor: $g \circ f = \mathbf{1}_A$, $f \circ g = \mathbf{1}_B$. Dacă există, inversa lui f se notează f^{-1}.

3.16 Propoziție. *Fie $f : A \to B$ şi $g : B \to C$ funcții. Atunci:*
a) f este inversabilă $\Leftrightarrow$ f este bijectivă;
b) $g \circ f$ este bijectivă $\Rightarrow$ g este surjectivă şi f este injectivă;
c) Compunerea a două funcții injective (*surjective*) *este funcție injectivă* (*surjectivă*). □

Definiția produsului cartezian poate fi extinsă prin recurență la o familie de trei sau mai multe mulțimi, sau, mai general, la o familie oarecare de mulțimi:

3.17 Definiție. a) Fiind date mulțimile A_1, A_2, A_3 [15], definim produsul lor cartezian:

$$A_1 \times A_2 \times A_3 := (A_1 \times A_2) \times A_3.$$

Astfel, $\forall a_1 \in A_1$, $\forall a_2 \in A_2$, $\forall a_3 \in A_3$, notăm $((a_1, a_2), a_3)$, mai simplu, cu (a_1, a_2, a_3).

b) Pentru orice $n \geq 3$ şi orice familie de n mulțimi $A_1, A_2, \ldots, A_n$, definim (prin recurență[16]):

$$A_1 \times A_2 \times \ldots \times A_n := (A_1 \times A_2 \times \ldots \times A_{n-1}) \times A_n.$$

$A_1 \times A_2 \times \ldots \times A_n$ se mai notează cu $\prod_{i=1}^{n} A_i$ sau $\prod_{1 \leq i \leq n} A_i$. Dacă $\forall i \in \{1,2, \ldots, n\}$, $a_i \in A_i$, se notează $((a_1, a_2, \ldots, a_{n-1}), a_n) \in \prod_{i=1}^{n} A_i$ cu $(a_1, a_2, \ldots, a_n)$. Astfel,

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i,\ i = \overline{1,n}\}$$

În cazul $A_1 = A_2 = \ldots = A_n = A$, $A \times A \times \ldots \times A$ (de n ori) se notează cu A^n.

c) Este necesară şi o definiție în cazul general al unei familii de mulțimi $(A_i)_{i \in I}$ indexată după o mulțime de indici I. Se defineşte produsul cartezian $\prod_{i \in I} A_i$:

$$\prod_{i \in I} A_i := \{\varphi : I \to \bigcup_{i \in I} A_i \mid \varphi(i) \in A_i,\ \forall i \in I\}.$$

3.18 Observație. Produsul cartezian definit ca la c), în cazul unei familii finite de mulțimi, nu este acelaşi cu cel definit la a) şi b) şi la **3.5**. Există însă o bijecție naturală între mulțimile obținute prin cele două definiții. De exemplu, dacă $I = \{1, 2\}$, avem funcția bijectivă β, definită pe $\{\varphi : \{1, 2\} \to A_1 \cup A_2 \mid \varphi(i) \in A_i,\ \forall i \in I\}$ cu valori în $A_1 \times A_2$, dată de $\beta(\varphi) = (\varphi(1), \varphi(2))$. Se pot astfel identifica noțiunile de produs cartezian definite mai sus.

Definim următoarele *tipuri remarcabile de relații pe o mulțime*:

3.19 Definiție. Fie o mulțime nevidă A şi ρ o relație pe A. Spunem că ρ este:
- *reflexivă* dacă $a\rho a$, $\forall a \in A$. Formal: $(\forall a)(a \in A \to a\rho a)$;

---

[15] În această ordine! De fapt, se dă o *familie de mulțimi* indexată după $\{1,2,3\}$.
[16] Folosim deocamdată o accepție intuitivă a noțiunii de definiție prin recurență. Pentru o tratare riguroasă, vezi **4.20** şi următoarele.

- *ireflexivă* dacă $\forall a \in A$, *nu* are loc $a\rho a$;
- *simetrică* dacă $\forall a, b \in A, a\rho b \to b\rho a$;
- *asimetrică* dacă $\forall a, b \in A, a\rho b \to \neg b\rho a$;
- *antisimetrică* dacă $\forall a, b \in A, a\rho b$ şi $b\rho a \to a = b$;
- *tranzitivă* dacă $\forall a, b, c \in A, a\rho b$ şi $b\rho c \to a\rho c$;
- *relație de echivalență* dacă este reflexivă, simetrică şi tranzitivă. Pentru relații de echivalență se folosesc notații de tipul $a \equiv b$, $a \sim b$ în loc de $a\rho b$.
- *relație de preordine* dacă este reflexivă şi tranzitivă;
- *relație de ordine* dacă este reflexivă, tranzitivă şi antisimetrică. Pentru relații de (pre)ordine se folosesc în general notații de tipul $a \le b$ în loc de $a\rho b$.
- *relație de ordine strictă* dacă este ireflexivă şi tranzitivă. Pentru relații de ordine strictă se folosesc în general notații de tipul $a < b$ în loc de $a\rho b$.

Relațiile de *ordine* şi de *echivalență* sînt deosebit de importante în toată matematica şi este esențială o bună cunoaştere a proprietăților lor.

3.20 Exercițiu. a) Scrieți formal condițiile de mai sus referitoare la o relație ρ.

b) Cum se generalizează definițiile anterioare la *relații* (în sensul de expresii cu două variabile libere)? De exemplu, o relație $R(x, y)$ se numeşte reflexivă dacă $(\forall x)R(x, x)$.

c) Exprimați definițiile de mai sus în termeni de incluziuni şi compuneri de relații (şi eventual de inverse). De exemplu, ρ este reflexivă înseamnă că $id_A \subseteq \rho$; ρ este simetrică înseamnă că $\rho^{-1} \subseteq \rho$.

Dacă $\le$ este o relație de ordine pe A, scriem $(A, \le)$ şi spunem că $(A, \le)$ este *mulțime ordonată*. Dacă pentru orice $a, b \in A$ avem $a \le b$ sau $b \le a$, atunci $(A, \le)$ se numeşte mulțime *total ordonată* (sau *lanț*) şi relația $\le$ se numeşte relație de *ordine totală*. Uneori, pentru a sublinia că o anumită relație de ordine nu este totală, se spune *relație de ordine parțială*. În loc de $a \le b$ se scrie şi $b \ge a$. Se observă că, dacă $\le$ este o relație de ordine pe A, atunci $\ge$ este tot o relație de ordine.

3.21 Observație. Dacă $\le$ este o relație de ordine pe A, atunci relația $<$ pe A, definită prin: $x < y \leftrightarrow (x \le y \wedge x \ne y)$ este o relație de *ordine strictă* pe A. Reciproc, dacă $<$ este o ordine strictă pe A, atunci, definind $x \le y \leftrightarrow (x < y \vee x = y)$ se obține o relație de ordine pe A. Verificați! Aşadar, există o bijecție între relațiile de ordine pe A şi relațiile de ordine strictă pe A. De aceea, orice definiție sau rezultat aplicabil unei relații de ordine se aplică şi relației de ordine strictă asociate (şi reciproc). Cum trebuie adaptate aceste considerații la *relațiile* văzute în sensul de la **3.8**?

3.22 Definiție. Fie $(A, \le)$ o mulțime ordonată şi B o submulțime a lui A. Un element $m \in A$ se numeşte *minorant* al lui B dacă $m \le b$, $\forall b \in B$. Un element $M \in A$ se numeşte *majorant* al lui B dacă $b \le M$, $\forall b \in B$. Submulțimea B se numeşte *minorată* (resp. *majorată*) dacă are un

minorant (resp. majorant). Dacă B conține un minorant m pentru B, spunem că m este *cel mai mic element* (sau *primul element*) *al lui B*. Dacă B conține un majorant M pentru B, M se numeşte *cel mai mare element* (sau *ultimul element*) *al lui B*.

Dacă B are un prim element $m \in B$*, acesta este unic*: $\forall m' \in B$, avem $m \le m'$ (m este prim element) şi $m' \le m$, deci $m = m'$ din antisimetrie. La fel, *ultimul element al lui B este unic* (*dacă există*).

Ca exercițiu, exprimați definițiile şi proprietățile de mai sus (date pentru relații de ordine) pentru relații de ordine *strictă*.

3.23 Exemplu. Relația de divizibilitate "|" pe $\mathbb{N}$, dată de:

$$\forall a, b \in \mathbb{N} \ \ (a|b \leftrightarrow \exists c \in \mathbb{N} \text{ astfel încît } b = ac)$$

este o relație de ordine, care *nu este totală* (nu are loc nici 2|3, nici 3|2); 0 *este ultimul element* al lui $(\mathbb{N}, |)$ şi 1 *este primul element* al lui $(\mathbb{N}, |)$. Relația uzuală de ordine "≤" pe $\mathbb{N}$ este *totală*, 0 este primul element al lui $(\mathbb{N}, \le)$; nu există ultimul element al lui $(\mathbb{N}, \le)$.

O mulțime $(A, \le)$ cu proprietatea că orice submulțime nevidă B a lui A are un prim element se numeşte mulțime *bine ordonată* (caz în care relația $\le$ pe A se numeşte *relație de bună ordine*). Mulțimile bine ordonate sînt foarte importante: pe o mulțime bine ordonată se poate aplica un raționament prin *inducție*.

Orice mulțime bine ordonată este total ordonată (demonstrați!).

3.24 Definiție. Un element m al unei mulțimi ordonate $(A, \le)$ se numeşte *element maximal* al lui A dacă, $\forall b \in A$ cu $m \le b$ rezultă $m = b$. Un element m se numeşte *element minimal* al lui A dacă, $\forall b \in A$ cu $b \le m$ rezultă $m = b$. De exemplu, în mulțimea ordonată $\mathbb{N} \setminus \{0, 1\}$ cu divizibilitatea, 2 este element minimal. Care sînt toate elementele sale minimale?

3.25 Definiție. Fie $(A, \le)$ o mulțime ordonată şi B o submulțime a sa. Fie $Maj(B)$ mulțimea majoranților lui B. Dacă există cel mai mic element al lui $Maj(B)$, acest element se numeşte *supremumul* (sau *marginea superioară a*) lui B şi se notează $\sup B$. Dacă există $\sup B = c$, atunci c este „*cel mai mic majorant al lui B*”, adică satisface condițiile:

- $\forall b \in B$, $b \le c$ (c este majorant al lui B).
- $\forall c' \in A$ astfel încît $\forall b \in B$, $b \le c'$, rezultă $c \le c'$ (c este mai mic decît orice alt majorant c' al lui B).

„Dual” (considerînd relația de ordine $\ge$) se obține noțiunea de *infimum* (sau *margine inferioară*) al submulțimii B a lui $(A, \le)$, notat (dacă există!) cu $\inf B$.

O mulțime ordonată $(A, \le)$ cu proprietatea că orice submulțime cu două elemente a sa are supremum şi infimum se numeşte *latice*. Dacă orice submulțime a lui A are sup şi inf, A se numeşte *latice completă*.

De exemplu, pentru o mulţime nevidă oarecare M, mulţimea $\mathcal{P}(M)$ a părţilor lui M este ordonată de relaţia de incluziune; dacă $A, B \in \mathcal{P}(M)$, atunci $\sup\{A, B\} = A \bigcup B$, $\inf\{A, B\} = A \bigcap B$. $(\mathcal{P}(M), \subseteq)$ este chiar o latice completă. La fel, $(\mathbb{N}, |)$ este o latice.

În $\mathbb{R}$, ordonat cu ordinea uzuală, orice submulţime nevidă majorată are supremum (aceasta este o proprietate fundamentală a lui $\mathbb{R}$, esenţială în Analiză). În $\mathbb{Q}$, nu orice submulţime nevidă are supremum (justificaţi!).

I.4. Ordinale, axioma infinităţii şi mulţimea numerelor naturale

În toată matematica este esenţială mulţimea numerelor naturale $\mathbb{N}$. Se pune problema unui mod de a construi această mulţime (sau, fiind vorba de un concept care poate apărea drept primar, de a axiomatiza $\mathbb{N}$). Vom arăta că, în cadrul teoriei axiomatice a mulţimilor, se poate da o construcţie satisfăcătoare a lui $\mathbb{N}$. Mai mult, modul de construcţie duce la o generalizare posibilă a mulţimii $\mathbb{N}$, sub forma *clasei ordinalelor*.

O modalitate de abordare a introducerii lui $\mathbb{N}$ este dată de *axiomatica Dedekind-Peano*. *Noţiunile primare* sînt cele de *număr natural* şi *funcţie succesor*[17]. Limbajul acestei teorii axiomatice este format din:

- simbolul = (notează egalitatea a două obiecte);
- simbolul 0 (notează un număr natural privilegiat fixat);
- nume variabile, constante, conectorii logici (ca la limbajul teoriei axiomatice a mulţimilor), cu deosebirea că numele denumesc acum obiectele acestei teorii, adică *numere naturale*.

Axiomele acestei teorii sînt:

1. Există un număr natural notat 0.

2. Pentru orice număr natural n, există un număr natural unic determinat, numit *succesorul lui n* şi notat $s(n)$ sau n^+: $(\forall n)(\exists n^+)$.

3. Orice două numere naturale cu acelaşi succesor sînt egale: $(\forall m)(\forall n)(m^+ = n^+ \rightarrow m = n)$.

4. 0 nu este succesorul nici unui număr natural: $(\forall n)(n^+ \neq 0)$.

5. (**Axioma inducţiei**) Pentru orice predicat cu o variabilă $A(n)$ are loc:

$$[A(0) \wedge (\forall n)(A(n) \rightarrow A(n^+)] \rightarrow (\forall m)A(m).$$

[17] Întrucît este vorba de o teorie axiomatică, funcţia succesor nu este a priori o *funcţie* în sensul teoriei mulţimilor (ci este o noţiune primară); este adevărat însă că în *modelul* pe care îl construim, rolul funcţiei succesor va fi jucat de o funcţie în sens uzual.

Observăm că axioma **5** (binecunoscutul *principiu de demonstrație prin inducție*) este de fapt o *schemă de axiome*.

Introducerea operațiilor cu numere naturale, a relației de ordine şi deducerea principalelor proprietăți ale acestora folosind axiomatica Dedekind-Peano sînt interesante şi instructive. Aceste aspecte fiind însă destul de cunoscute (vezi de ex. BECHEANU et al. [1983]), nu insistăm în această direcție. Vom arăta, în schimb, că se poate *modela* sistemul axiomatic de mai sus în cadrul teoriei mulțimilor, dacă mai introducem o axiomă (de fapt, acest *model* se expune în general, cînd se vorbeşte de axiomatica Peano). Mai precis, vom construi o *mulțime* $\mathbb{N}$, un *element* $0 \in \mathbb{N}$ şi o *funcție* (în sens uzual) $s : \mathbb{N} \to \mathbb{N}$, $s(n) = n^+$, care să satisfacă axiomele de mai sus.

Începem cu o abordare intuitivă. Instrumentele oferite pînă acum de axiomele teoriei mulțimilor permit considerarea următorului „şir de mulțimi”:

$$\varnothing;\ \{\varnothing\};\ \{\varnothing, \{\varnothing\}\};\ \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\};\ \ldots \qquad (1)$$

Se observă că, pentru fiecare termen x al şirului, următorul termen este $x \bigcup \{x\}$. Primul termen are 0 elemente, al doilea are 1 element ş.a.m.d. Ar fi tentant să considerăm drept mulțime a numerelor naturale „mulțimea tuturor termenilor acestui şir”, $\varnothing$ să joace rolul lui 0, iar funcția succesor să fie $s(x) = x \bigcup \{x\}$. Apar două probleme: *definirea riguroasă* a „mulțimii tuturor termenilor şirului (1)” şi garantarea *existenței* unei astfel de mulțimi. Faptul că există o mulțime care *include* toți termenii şirului (1) este asigurat de o nouă axiomă:

4.1 Axioma infinității. $(\exists M)\ [\varnothing \in M \wedge (\forall y)(y \in M \to y \bigcup \{y\} \in M)]$.

Intuitiv, este clar că axioma de mai sus garantează existența unei mulțimi M care să conțină toate mulțimile şirului (1); aceasta nu înseamnă că M conține *doar* aceste mulțimi. Vom adopta următoarea strategie: definim riguros *clasa* mulțimilor din şirul (1) (aceasta va fi clasa *ordinalelor finite*, noțiune pe care o vom defini în cele ce urmează); atunci mulțimea $\mathbb{N}$ a numerelor naturale va fi obținută prin comprehensiune, ca fiind mulțimea acelor elemente din M (dată de axioma infinității) care sînt în plus ordinale finite. Apoi demonstrăm că toate aceste obiecte satisfac axiomele Dedekind-Peano.

4.2 Definiție. O mulțime α se numeşte *ordinal* dacă are următoarele proprietăți:

i) α este *tranzitivă*, adică $(\forall x)(x \in \alpha \to x \subseteq \alpha)$.

ii) relația de apartenență defineşte o relație de *ordine strictă* pe α, care este o *bună ordine* pe α. Detaliind, această condiție este echivalentă cu:

- $\forall x, y, z \in \alpha$, din $x \in y$ şi $y \in z$ rezultă că $x \in z$ (*tranzitivitatea* relației $\in$);
- $\forall x, y \in \alpha$, din $x \in y$ rezultă că $y \notin x$ (*ireflexivitatea* relației $\in$);
- orice submulțime nevidă a lui α are un prim element (față de relația $\in$):

$$\forall \beta\ \{(\beta \subseteq \alpha \wedge \beta \neq \varnothing) \to \exists x\ [x \in \beta \wedge \forall y(y \in \beta \to (x = y \vee x \in y))]\}.$$

4.3 Exemplu. Orice element din şirul (1) este ordinal.

Clasa ordinalelor se notează cu *On*. Astfel, scrierea $On(\alpha)$ înseamnă „mulțimea α este un ordinal”.[18]

Înainte de a defini ordinalele *finite*, avem nevoie de unele pregătiri.

4.4 Definiție. Fie $(A, \leq)$ o mulțime ordonată. O submulțime S a lui A se numeşte *segment inițial* al lui A dacă are proprietatea că, odată cu un element x, conține toate elementele mai mici decît x: $\forall x\ [x \in S \rightarrow (\forall y\ (y \in A \wedge y \leq x\ ) \rightarrow y \in S]$.

De exemplu, dacă fixăm $a \in A$, mulțimea $S_a(A) := \{x \in A \mid x < a\}$ este un segment inițial în A. Este remarcabil că în mulțimi *bine ordonate*, toate segmentele inițiale sînt de acest tip:

4.5 Propoziție. *Fie $(A, \leq)$ o mulțime bine ordonată şi S un segment inițial al lui A. Atunci: sau $S = A$, sau există $a \in A$ astfel încît $S = S_a(A) := \{x \in A \mid x < a\}$.*

Demonstrație. Presupunem că $S \neq A$. Atunci $A \setminus S$ este nevidă şi (A fiind bine ordonată) are un prim element a. Afirmăm că $S_a(A) = S$. Într-adevăr, fie $x \in S$. Dacă $a \leq x$, atunci $a \in S$, din definiția segmentului inițial. Cum A este total ordonată, rezultă că $x < a$, adică $x \in S_a(A)$. Incluziunea cealaltă o lăsăm cititorului. □

4.6 Propoziție. *Fie α un ordinal şi s un segment inițial în α. Atunci $s = \alpha$ sau există $\beta \in \alpha$ astfel încît $s = \beta = S_\beta(\alpha)$.*

Demonstrație. Reamintim că relația de ordine strictă pe α este $\in$, față de care α este bine ordonată. Din propoziția precedentă rezultă că $s = \alpha$ sau există $\beta \in \alpha$ astfel încît $s = S_\beta(\alpha)$. Dar $S_\beta(\alpha) = \{x \in \alpha \mid x \in \beta\} = \alpha \cap \beta$. Cum α este ordinal, din $\beta \in a$ rezultă $\beta \subseteq \alpha$, deci $\alpha \cap \beta = \beta$. □

4.7 Propoziție. *Orice element al unui ordinal este tot un ordinal.*

Demonstrație. Fie α un ordinal şi $\beta \in \alpha$. Atunci $\beta = S_\beta(\alpha)$, care este un segment inițial în α. În general, orice submulțime nevidă a unei mulțimi bine ordonate A este bine ordonată de relația de ordine de pe A (demonstrați!), deci $\beta = S_\beta(\alpha)$ este bine ordonat de $\in$. Avem şi că β este tranzitivă: dacă $x \in \beta$, iar $y \in x$, atunci $x \in \alpha$ (căci $\beta \in \alpha$ şi α este tranzitivă). Acum, din $x \in \alpha$ şi $y \in x$ deducem că $y \in \alpha$. Am obținut că $y, x, \beta \in \alpha$, $y \in x$ şi $x \in \beta$. Relația $\in$ este tranzitivă pe α, deci $y \in \beta$. □

4.8 Propoziție. *Dacă α este un ordinal, atunci $\alpha \notin \alpha$.*

Demonstrație. Relația de apartenență $\in$ este de ordine strictă pe α, deci este ireflexivă: $\forall x \in \alpha$, avem $x \notin x$. Dacă presupunem că $\alpha \in \alpha$, obținem astfel că $\alpha \notin \alpha$, absurd. □

---

[18] Ideea de a defini ordinalele în această manieră îi aparține lui John von Neumann. Un ordinal se poate defini şi ca o *clasă de izomorfism de mulțimi bine ordonate.* În această abordare însă, clasa ordinalelor ar fi o "clasă de clase", o complicare tehnică evitată de prezentarea aleasă aici.

4.9 Propoziţie. *Pentru orice ordinale α şi β, are loc una şi numai una din afirmaţiile: $\alpha \in \beta$, $\alpha = \beta$ sau $\beta \in \alpha$.*

Demonstraţie. Fie $\gamma = \alpha \cap \beta = \{x \in \alpha \mid x \in \beta\}$. Se verifică imediat că γ este un segment iniţial în mulţimea ordonată $(\alpha, \in)$ (vezi def. **4.4**). Din **4.6** rezultă că $\gamma = \alpha$ sau $\gamma \in \alpha$. Simetric, avem $\gamma = \beta$ sau $\gamma \in \beta$. Analizăm toate posibilităţile: 1) $\gamma = \alpha$ şi $\gamma = \beta$. Atunci $\alpha = \beta$. 2) $\gamma = \alpha$ şi $\gamma \in \beta$. Atunci $\alpha \in \beta$. 3) $\gamma \in \alpha$ şi $\gamma = \beta$. Atunci $\beta \in \alpha$. 4) $\gamma \in \alpha$ şi $\gamma \in \beta$. Atunci $\gamma \in \alpha \cap \beta = \gamma$, imposibil: γ este ordinal şi s-ar contrazice **4.8**.

Cele trei situaţii din enunţ sînt mutual incompatibile: dacă $\alpha \in \beta$, atunci $\alpha = \beta$ ar contrazice **4.8**, iar $\beta \in \alpha$ implică (pentru că α este tranzitivă) $\alpha \in \alpha$, aceeaşi contradicţie. □

Putem enunţa proprietatea de mai sus sub forma: *Clasa ordinalelor este total ordonată de relaţia de ordine strictă* $\in$.

Mai mult, *clasa ordinalelor este bine ordonată de relaţia de apartenenţă.* Acest enunţ necesită precizări: nu am definit încă noţiunea de *clasă* bine ordonată. O analogie directă cu *mulţimile* bine ordonate ar conduce la următoarea „definiţie": o clasă $C(x)$ ordonată de o relaţie (în sensul de la **3.8**) de ordine $R(x, y)$ este bine ordonată dacă *orice subclasă* nevidă a sa are un prim element. Sintagma *„orice subclasă"* inclusă în definiţie conduce de fapt la a da o *schemă* de definiţii, căci clasele nu sînt obiecte ale teoriei, ci expresii ale limbajului formal (cf. comentariul de la Axioma-schemă a substituţiei). Se adoptă următoarea definiţie, mai restrictivă, dar care nu are dezavantajul descris anterior:

4.10 Definiţie. O clasă $C(x)$ se numeşte *bine ordonată* de o relaţie de ordine strictă $R(x, y)$ dacă este total ordonată de R şi orice segment iniţial al lui C în raport cu relaţia R este o <u>mulţime</u> bine ordonată de R. Mai precis, au loc afirmaţiile:

- R este o relaţie ireflexivă pe C: $\forall x(C(x) \to \neg R(x, x))$.
- R este o relaţie tranzitivă pe C: $\forall x\ \forall y\ \forall z(C(x) \wedge C(y) \wedge C(z) \wedge R(x,y) \wedge R(y,z) \to R(x, z))$.
- R este o relaţie totală pe C: $\forall x\ \forall y\ (C(x) \wedge C(y) \to (R(x, y) \vee R(y, x) \vee x = y))$.
- Pentru orice mulţime t, segmentul iniţial al clasei C determinat de t în raport cu relaţia R, adică clasa $S_t(C)(\text{mod } R) := C(x) \wedge R(x, t)$, este o *mulţime* bine ordonată de R:

$(\forall t)(\exists s)[(\forall x)(x \in s \leftrightarrow (C(x) \wedge R(x, t))] \wedge (\forall u)[(u \neq \varnothing \wedge u \subseteq s) \to \exists p(p$ primul element al lui $u)]$

Dacă C este bine ordonată de R în sensul definiţiei anterioare, atunci *orice clasă nevidă inclusă în C are prim element*. Într-adevăr, fie D o clasă nevidă inclusă în C şi fie t un element din D (adică $D(t)$ adevărată). Dacă t este prim element în D în raport cu R, atunci am terminat. Dacă nu, există q în D mai mic strict decît t: $D(q) \wedge R(q, t)$. Dar segmentul iniţial $S_t(C)(\text{mod } R)$ este o mulţime; deci intersecţia clasei D cu $S_t(C)(\text{mod } R)$, adică clasa $D(x) \wedge (x \in S_t(C)(\text{mod } R))$ este o submulţime S a lui $S_t(C)(\text{mod } R)$ (nevidă, căci conţine q). Din buna ordonare a lui $S_t(C)(\text{mod } R)$ deducem că există primul element m al mulţimii S. Acesta este primul element al clasei D: dacă ar exista n în D, mai mic decît m, atunci n este mai mic

decît t şi deci $n \in S_t(C)(\text{mod } R)$. Astfel, $n \in S$ şi obţinem o contradicţie cu faptul că m este primul element al lui S.

Să demonstrăm acum:

4.11 Propoziție. *Clasa ordinalelor On este bine ordonată de relația de apartenență.*

Demonstrație. Am văzut (**4.9**) că relația de apartenență este totală pe clasa ordinalelor. Fie α un ordinal şi segmentul inițial $S_\alpha(On)(\text{mod} \in) = On(t) \wedge (t \in \alpha)$. Evident, această clasă este o mulțime, anume α (orice element t al lui α este ordinal). Din definiția ordinalelor, α este bine ordonat de apartenență. □

Ordonarea „nestrictă" pe clasa *On* este *incluziunea*. Mai precis, pentru două ordinale α şi β, $(\alpha \in \beta \vee \alpha = \beta)$ este echivalent cu $\alpha \subseteq \beta$. Cel mai mic ordinal este $\varnothing$. Care este însă cel mai mic ordinal mai mare decît un ordinal α dat?

4.12 Propoziție. *Pentru orice ordinal α, $\alpha \bigcup \{\alpha\}$ este tot ordinal* (*numit* succesorul *lui* α) *şi este cel mai mic ordinal, mai mare decît α.*

Demonstrație. Propunem spre demonstrație afirmația: α ordinal implică $\alpha \bigcup \{\alpha\}$ ordinal. Fie acum β un ordinal mai mare decît α. Atunci $\alpha \in \beta$ (adică $\{\alpha\} \subseteq \beta$). Deci $\alpha \subseteq \beta$ (căci β ordinal), şi astfel $\alpha \bigcup \{\alpha\} \subseteq \beta$. Aceasta demonstrează că orice ordinal mai mare decît α este mai mare sau egal cu $\alpha \bigcup \{\alpha\}$. Pe de altă parte, este evident că $\alpha \in \alpha \bigcup \{\alpha\}$. □

4.13 Definiție. Dacă pentru ordinalul β există α astfel încît $\beta = \alpha \bigcup \{\alpha\}$ (β este succesorul lui α), atunci α este ordinal, unic determinat de β (de ce?) şi se numeşte *predecesorul* lui β. Un ordinal α se numeşte *ordinal finit* dacă: sau $\alpha = \varnothing$, sau orice element al lui α şi α însuşi au un predecesor. Un ordinal care nu este finit se numeşte *ordinal infinit*.

Se observă că toate mulțimile din şirul (1) sînt ordinale finite. De altfel, şirul a fost construit plecînd de la $\varnothing$ şi luînd succesorul fiecărui ordinal construit deja.

Dacă α este ordinal finit, atunci se verifică imediat că:

- orice ordinal $\beta \subseteq \alpha$ este ordinal finit.
- succesorul lui α, $\alpha \bigcup \{\alpha\}$, este ordinal finit.

4.14 Propoziție. *Axioma infinității este echivalentă cu afirmația:*

Ordinalele finite formează o mulțime (*notată cu* ω).

Demonstrație. Presupunem axioma infinității adevărată şi considerăm *mulțimea* $\omega := \{\alpha \in M \mid \alpha \text{ ordinal finit}\}$, unde M este dată de **4.1**. Să arătăm că ω conține orice ordinal finit. Dacă nu ar fi aşa, ar exista un ordinal finit β, cu $\beta \notin M$. Cum clasa ordinalelor finite este bine ordonată, există cel mai mic ordinal finit μ cu proprietatea că $\mu \notin M$. Cum $\varnothing \in M$, $\mu \neq \varnothing$. Însă atunci μ are un predecesor λ, care (din modul de alegere al lui μ) este în M. Însă atunci succesorul lui λ (adică μ) aparține lui M, contradicție.

Invers, dacă ordinalelele finite formează o mulţime ω, atunci ω satisface proprietăţile din axioma **4.1**: $\varnothing \in \omega$ şi $\forall \alpha \in \omega$, avem $\alpha \bigcup \{\alpha\} \in \omega$. □

Acum se poate da următorul **model** (în cadrul teoriei axiomatice a mulţimilor) pentru axiomele Dedekind-Peano:

- numerele naturale sînt *ordinalele finite*;
- numărul natural 0 este *mulţimea vidă* $\varnothing$;
- funcţia succesor este funcţia $s : \omega \to \omega$ care *asociază fiecărui ordinal finit* α *succesorul său* $\alpha \bigcup \{\alpha\}$.

Clar, axiomele **1-4** sînt verificate. Să verificăm şi axioma inducţiei:

4.15 Propoziţie. (*Teorema inducţiei pe mulţimea ordinalelor finite*) *Fie P o clasă de ordinale finite astfel încît* $P(\varnothing)$ *este adevărată şi,* $\forall \alpha$ *ordinal finit cu* $P(\alpha)$ *adevărată, rezultă că* $P(\alpha \bigcup \{\alpha\})$ *adevărată. Atunci* $P(\alpha)$ *adevărată pentru orice ordinal finit* α.

Demonstraţie. Clasa P corespunde unei submulţimi (notată tot P) a lui ω. Dacă $P \neq \omega$, atunci $\omega \setminus P \neq \varnothing$ şi deci $\omega \setminus P$ are un prim element β, cu $\beta \neq \varnothing$ din ipoteza $P(\varnothing)$ adevărată. Fie α predecesorul lui β. Avem $\alpha \notin \omega \setminus P$, deci $P(\alpha)$ adevărată, de unde rezultă $P(\alpha \bigcup \{\alpha\}) = P(\beta)$ adevărată, adică $\beta \in P$, contradicţie cu $\beta \in \omega \setminus P$. □

4.16 Observaţie. Mulţimea ω a ordinalelor finite este un ordinal (demonstraţi!), care nu este finit.

Alte rezultate despre ordinale sînt propuse ca exerciţii. Detalii şi dezvoltări ale teoriei ordinalelor pot fi găsite de exemplu în SCORPAN [1996].

În continuare vom identifica mulţimea ordinalelor finite ω cu mulţimea numerelor naturale $\mathbb{N}$. Notăm cu $\leq$ relaţia de ordine pe $\mathbb{N}$ (numită relaţia de ordine uzuală) şi cu $n + 1$ succesorul numărului natural (ordinalului finit) n. Prin această identificare, 0 corespunde lui $\varnothing$, 1 lui $\{\varnothing\}$, ş.a.m.d.; $n + 1$ corespunde lui $n \bigcup \{n\}$. Observăm că atunci $n = \{0, 1, \ldots, n - 1\}$.

Prin analogie cu $\mathbb{N}$, se notează cu $<$ relaţia de ordine strictă pe *On* (pentru orice ordinale α, β, $\alpha < \beta$ înseamnă deci $\alpha \in \beta$) şi cu $\alpha + 1$ succesorul ordinalului α (deci $\alpha + 1 = \alpha \bigcup \{\alpha\}$).

Este deosebit de important următorul enunţ, care stă la baza raţionamentelor prin inducţie:

Mulţimea numerelor naturale $\mathbb{N}$ *este bine ordonată în raport cu relaţia de ordine uzuală.*

Considerăm utile cîteva remarci şi rezultate privind tehnica de *demonstraţie prin inducţie*, respectiv de *definire prin recurenţă*. Mai întîi dăm un rezultat care este cunoscut uneori ca o „variantă a principiului de inducţie”:

4.17 Propoziţie. *Fie* $P(x)$ *o expresie cu proprietatea că, pentru orice număr natural n, dacă* $P(k)$ *este adevărată pentru orice* $k < n$*, rezultă că* $P(n)$ *este adevărată. Atunci* $P(n)$ *este*

adevărată pentru orice număr natural n. Mai precis, are loc (*subînţelegem că toate variabilele sînt în* $\mathbb{N}$):

$$\{\forall n\ [(\forall k\ (k < n \to P(k)) \to P(n)]\} \to (\forall n)(P(n)).$$

Demonstraţie. Mai întîi observăm că, în condiţiile din enunţ, $P(0)$ este adevărată. Într-adevăr, pentru $n = 0$ are loc implicaţia: $[\forall k(k < 0 \to P(k)] \to P(0)$. Dar $\forall k(k < 0 \to P(k))$ este adevărată, deoarece $k < 0$ este falsă pentru orice $k \in \mathbb{N}$ (o expresie de forma $p \to q$ este adevărată dacă p este falsă!). Deci $P(0)$ adevărată. [19]

Presupunem prin absurd că există $n \in \mathbb{N}$ astfel încît $P(n)$ să fie falsă. Atunci mulţimea nevidă $\{n \in \mathbb{N} \mid P(n) \text{ falsă}\}$ are un prim element a. Deci $P(k)$ este adevărată, $\forall k < a$, din modul de alegere a lui a. Cum are loc implicaţia $(\forall k(k < a \to P(k)) \to P(a)$, rezultă că $P(a)$ este adevărată, absurd. □

Este remarcabil faptul că acest rezultat are loc în *orice mulţime bine ordonată.* Propunem cititorului să reia ideea demonstraţiei de mai sus pentru a arăta :

4.18 Propoziţie. *Fie* $(A, \le)$ *o mulţime bine ordonată şi fie* $P(x)$ *o expresie cu proprietatea că, pentru orice* $n \in A$, *dacă* $P(k)$ *este adevărată pentru orice* $k < n$, $k \in A$, *rezultă că* $P(n)$ *adevărată. Atunci* $P(n)$ *adevărată pentru orice* $n \in A$. *Mai precis, are loc* (*subînţelegem că toate variabilele sînt în* A):

$$\{\forall n\ [(\forall k\ (k < n \to P(k)) \to P(n)]\} \to (\forall n)(P(n)).$$ □

Un exemplu de aplicare a acestei propoziţii este demonstraţia teoremei polinoamelor simetrice (unde mulţimea bine ordonată este $\mathbb{N}^n$, cu ordinea lexicografică).

Mai mult, se poate face inducţie pe *clase bine ordonate*. Dacă $R(x, y)$ este o relaţie de ordine, vom scrie, mai sugestiv, $x < y \pmod R$ în loc de $R(x, y) \wedge (x \ne y)$. Demonstraţia rezultatului ce urmează este similară cu cea de la mulţimi bine ordonate.

4.19 Propoziţie. *Fie* $A(x)$ *o clasă bine ordonată de o relaţie* $R(x, y)$ *şi fie* $P(x)$ *o expresie cu proprietatea că, pentru orice n din clasa A, dacă* $P(k)$ *este adevărată pentru orice k din A, cu* $k < n \pmod R$, *rezultă că* $P(n)$ *adevărată. Atunci* $P(n)$ *adevărată pentru orice n din A. Mai precis, dacă are loc*:

$$\forall n\{[A(n) \wedge (\forall k\ (A(k) \wedge k < n (\mathrm{mod}\ R)) \to P(k)] \to P(n)\},$$

atunci are loc $(\forall n)(A(n) \to P(n))$. □

În general, astfel de raţionamente se fac pe *clasa ordinalelor On* şi se numesc raţionamente prin *inducţie transfinită*.

Strîns legat de principiul demonstraţiei prin inducţie este *definirea şirurilor prin recurenţă* (numită uneori *definire prin inducţie*, denumire improprie, căci inducţia este o metodă de

[19] Aşadar, nu are rost să se arate că $P(0)$ este adevărată cînd se foloseşte acest raţionament prin inducţie!

demonstraţie). De exemplu, este clar că relaţiile $x_0 = 1$, $x_{n+1} = 2x_n + 1$, $\forall n \in \mathbb{N}$, definesc unic şirul de numere naturale: $x_0 = 1$, $x_1 = 3$, $x_2 = 7$, $x_3 = 15$, … .

4.20 Definiţie. Fie A o mulţime nevidă. Se numeşte *şir* (indexat după ω)[20], cu valori în A, orice funcţie $s : \omega \to A$ (ω este ordinalul tuturor ordinalelor finite). Mai general, dacă α este un ordinal oarecare, vom numi *şir* (indexat după α) cu valori în A orice funcţie definită pe α cu valori în A.

Pentru un şir $s : \alpha \to A$ se folosesc notaţii de tipul $(s_i)_{i\in\alpha}$ sau $\{s_i \mid i \in \alpha\}$. Pentru orice $\beta \in \alpha$ (β este deci ordinal!), notăm cu $s|_\beta$ restricţia lui s la β ($s|_\beta$ este atunci şir indexat după β). De exemplu, dacă $(s_n)_{n\in\omega}$ este un şir indexat după ω, atunci:

$s|_0 = s|_\varnothing = \varnothing$; $s|_1 = s|_{\{0\}} = \{(0, s(0))\}$; $s|_2 = s|_{\{0,1\}} = \{(0, s(0)), (1, s(1))\}$, …,
$s|_n = s|_{\{0,1,\, \dots,\, n-1\}} = \{(0, s(0)), (1, s(1)), \dots, (n-1, s(n-1))\}$.

Ce înseamnă a *defini prin recurenţă* un şir $(s_n)_{n\in\omega}$? Intuitiv, pentru orice $n \in \omega$, termenul s_n „depinde de termenii precedenţi $s_0, \dots, s_{n-1}$”, adică este dată o „relaţie de recurenţă” de forma $s_n = f(s_0, \dots, s_{n-1})$. Observăm că putem rescrie aceasta sub forma $s_n = f(s|_n)$, folosind notaţiile de mai sus. Deci f este o funcţie cu domeniul format de mulţimea şirurilor (cu valori în A), indexate după un $n = \{0,1, \dots, n-1\}$. Mai general, putem da următoarea:

4.21 Definiţie. Fie A o mulţime nevidă şi α un ordinal. Pentru fiecare $\beta \in \alpha$ notăm cu

$$S_\beta(A) = \{b \mid b : \beta \to A\}$$

mulţimea şirurilor cu valori în A, indexate după β. Fie

$$S(A, \alpha) = \bigcup_{\beta \in \alpha} S_\beta(A) = \{b \mid (\exists\beta)\ (\beta \in \alpha \text{ şi } b \text{ este funcţie de la } \beta \text{ la } A)\}$$

mulţimea şirurilor cu valori în A, indexate după ordinale din α. Dacă $s : \alpha \to A$ şi $\beta \in \alpha$, atunci $s|_\beta \in S_\beta(A) \subseteq S(A, \alpha)$, deci există $f(s|_\beta) \in A$.

O *relaţie de recurenţă* este o funcţie $f : S(A, \alpha) \to A$. Spunem că şirul $s : \alpha \to A$ este *definit recurent de relaţia de recurenţă* f dacă, $\forall\beta \in \alpha$, avem :

$$s(\beta) = f(s|_\beta).$$

4.22 Teoremă. *Fie α un ordinal şi A o mulţime. Pentru orice relaţie de recurenţă $f : S(A, \alpha) \to A$ există un unic şir $s : \alpha \to A$ care este definit recurent de f.*

Demonstraţie. Unicitatea: presupunem că există două şiruri $s : \alpha \to A$ *şi* $t : \alpha \to A$, definite recurent de f, astfel încît $s \neq t$. Deci mulţimea $\{\beta \in \alpha \mid s(\beta) \neq t(\beta)\}$ este nevidă şi are un prim element π. Atunci $s(\gamma) = t(\gamma)$, $\forall\gamma \in \pi$, adică $s|_\pi = t|_\pi$. Dar $s(\pi) = f(s|_\pi) = f(t|_\pi) = t(\pi)$, contradicţie.

[20] Reamintim că am identificat $\mathbb{N}$ cu ordinalul ω.

Existența: Notăm cu δ mulțimea ordinalelor β din α pentru care există un şir s_β indexat după β, definit recurent de f, adică: $\delta := \{\beta \in \alpha \mid \exists\ s_\beta : \beta \to A \wedge (\forall \gamma \in \beta \ \to\ s_\beta(\gamma) = f(s_\beta|_\gamma))\}$. Evident, $\delta \subseteq \alpha$. Avem de arătat că $\delta = \alpha$.

Afirmăm că *δ este un ordinal*. E suficient să demonstrăm că δ este segment inițial (vezi **4.6**). Observăm că $\varnothing \in \delta$ (funcția $\varnothing : \varnothing \to A$ este definită recurent de f!), deci δ este nevidă. Fie $\beta \in \delta$. Vrem să arătăm că $\gamma \in \delta$, $\forall \gamma < \beta$. Cum $\beta \in \delta$, există $s : \beta \to A$ definit recurent de f. Pentru $s|_\gamma$ avem, $\forall \lambda \in \gamma : s|_\gamma(\lambda) = s(\lambda) = f(s|_\lambda) = f((s|_\gamma)|_\lambda)$, deci $s|_\gamma$ este definit pe γ şi este definit recurent de f. Astfel, $\gamma \in \delta$.

Cum δ este ordinal şi $\delta \subseteq \alpha$, avem $\delta = \alpha$ sau $\delta \in \alpha$. Dacă $\delta = \alpha$, am terminat. Presupunem prin absurd că $\delta \in \alpha$.

Observăm că, $\forall \beta \in \delta$, şirul s_β definit recurent de f este unic determinat, din prima parte a demonstrației. Mai mult, $\forall \beta \in \delta$ şi $\forall \gamma \in \beta$, restricția lui s_β la γ coincide cu s_γ (tot din unicitate). Definim atunci $s : \delta \to A$ prin : $\forall \beta \in \delta$, $s(\beta) = f(s_\beta)$. Definiția are sens: s_β este un şir indexat după β (unicul şir definit recurent pe β de f) şi există $f(s_\beta) \in A$.

Să demonstrăm că $s : \delta \to A$ este definit recurent pe δ de f, adică: $\forall \beta \in \delta$ are loc $s(\beta) = f(s|_\beta)$. Comparînd cu definiția lui s, aceasta revine la a arăta că $\forall \beta \in \delta$, avem $s|_\beta = s_\beta$.

Fie $\beta \in \delta$ şi fie $\gamma \in \beta$. Avem, din cele de mai sus: $s(\gamma) = f(s_\gamma) = f(s_\beta|_\gamma) = s_\beta(\gamma)$, $\forall \gamma \in \beta$. Deci $s|_\beta(\gamma) = s_\beta(\gamma)$, $\forall \gamma \in \beta$, adică $s|_\beta = s_\beta$.

Deci $\delta \in \alpha$ şi există $s : \delta \to A$ definit recurent de f. Din definiția lui δ, avem $\delta \in \delta$; absurd.□

Definițiile prin recurență pe un ordinal oarecare sînt cunoscute ca definiții prin *recurență transfinită*. Acest tip de definiții se utilizează, între altele, în teoria dimensiunii laticelor şi a modulelor (vezi de exemplu NĂSTĂSESCU [1983]).

Prezentăm o proprietate foarte importantă a lui $\mathbb{N}$, a cărei demonstrație ilustrează principiul de demonstrație prin inducție. Se presupun cunoscute operațiile de adunare şi înmulțire în $\mathbb{N}$ şi proprietățile lor.

4.23 Teoremă (Teorema împărțirii cu rest în $\mathbb{N}$). *Pentru orice numere naturale a, b, cu* $b \neq 0$*, există q,* $r \in \mathbb{N}$ *astfel încît* $a = bq + r$ *şi* $r = 0$ *sau* $r < b$ (*q se numeşte* cîtul *iar r* restul *împărțirii lui a la b*). *În plus, q şi r sînt unic determinate cu aceste proprietăți.*

Demonstrație. Fie $b \neq 0$ fixat. Demonstrăm prin inducție după a, aplicînd **4.17**. Mai precis, considerăm $P(a)$: $\exists q\ \exists r\ (q \in \mathbb{N} \wedge r \in \mathbb{N} \wedge a = bq + r \wedge r < b)$.

Pentru orice $a < b$, $P(a)$ este adevărată, luînd $q = 0$, $r = a$. Presupunem acum că $a \geq b$ şi $P(k)$ este adevărată, $\forall k \in \mathbb{N}$, $k < a$. Să demonstrăm $P(a)$. Cum $a \geq b$ avem $a - b \in \mathbb{N}$ şi $a - b < a$. Deci are loc $P(a - b)$: $\exists q, r$ astfel încît $a - b = bq + r$ şi $r < b$, adică $a = b(q + 1) + r$, cu $r < b$.

Unicitatea: presupunem că $a = bq + r = bt + s$, cu $r < b$ şi $s < b$. Pentru a face o alegere, fie $q \geq t$, adică $q - t \geq 0$. Atunci $b(q - t) = s - r$. Cum $s < b$, rezultă că $s - r < b$. Astfel, $b(q - t) < b$, de unde obținem $q - t = 0$ şi $s - r = 0$. □

Teorema împărțirii cu rest este de o importanță covîrşitoare în matematică. O primă aplicație a ei este *reprezentarea numerelor naturale într-o bază dată* (vezi Exerciții).

Un alt punct de vedere privind ordinalele este descris în continuare.

4.24 Definiție. Fie $(A, \leq)$ şi $(B, \leq)$ mulțimi ordonate. O aplicație $\varphi : A \to B$ se numeşte *morfism de ordine* (sau *aplicație crescătoare*) dacă $\forall x, y \in A$, din $x \leq y$ rezultă $\varphi(x) \leq \varphi(y)$. Morfismul φ se numeşte *izomorfism de ordine* dacă φ este bijectivă şi inversa sa φ^{-1} este tot morfism. Mulțimile ordonate $(A, \leq)$ şi $(B, \leq)$ se numesc *izomorfe* dacă există măcar un izomorfism de ordine $\varphi : A \to B$, caz în care scriem $A \cong B$.

4.25 Observație. Dacă $(A, \leq)$ şi $(B, \leq)$ sînt *total* ordonate, atunci orice morfism bijectiv $\varphi : A \to B$ este şi izomorfism. Demonstrați! Pentru mulțimi ordonate în general, nu orice morfism bijectiv este izomorfism, după cum arată exemplul aplicației identitate id : $(\mathbb{N}^*, |) \to (\mathbb{N}^*, \leq)$, unde $(\mathbb{N}^*, |)$ este mulțimea numerelor naturale nenule înzestrată cu relația de ordine divizibilitatea, iar $\leq$ este relația de ordine uzuală.

Comparați rezultatul următor cu **4.9**:

4.26 Propoziție. *Fie A şi B mulțimi <u>bine ordonate</u>. Atunci are loc exact una din situațiile: $A \cong B$; A izomorf cu un segment inițial al lui B; B izomorf cu un segment inițial al lui A.* □

Clasa mulțimilor ordonate izomorfe cu o mulțime ordonată dată $(A, \leq)$ se numeşte *tipul de ordine* al lui $(A, \leq)$. Orice mulțime bine ordonată este izomorfă cu un unic ordinal:

4.27 Propoziție. *Fie $(A, \leq)$ o mulțime bine ordonată. Atunci există un unic ordinal $(\alpha, \in)$ izomorf cu $(A, \leq)$.* □

Astfel, pentru orice tip de *bună* ordine, există un unic ordinal în acel tip (şi, evident, orice ordinal se află într-un unic tip de bună ordine). Din acest motiv, uneori prin *ordinal* se înțelege *un tip de ordine de mulțimi bine ordonate*. Rezultatele enunțate arată echivalența celor două abordări.

I.5. Comentarii şi completări privind axiomatica mulțimilor

În această secțiune vom discuta cu titlu informativ anumite aspecte ale teoriei axiomatice a mulțimilor. Pentru detalii, se pot consulta lucrări precum SCORPAN [1996], MANIN [1977].

Sistemul ZF propriu-zis conține 4 axiome şi o schemă de axiome: *axioma extensionalității, axioma reuniunii, axioma mulțimii părților, schema de axiome a substituției* şi *axioma infinității.*

Este de dorit ca orice teorie axiomatică (deci şi ZF) să satisfacă următoarele proprietăţi:

Consistenţa (sau *necontradictorietatea*) teoriei: din axiomele teoriei nu se poate deduce simultan o propoziţie şi negaţia ei (adică nu se poate obţine o *contradicţie*). O teorie care nu este consistentă nu are nici o valoare ştiinţifică: *dacă există o propoziţie p astfel încît p şi* $\neg p$ *sînt adevărate, atunci orice propoziţie q este adevărată* (ceea ce elimină orice interes în stabilirea adevărului unei propoziţii). Într-adevăr, este clar că, dacă p şi $p \to q$ sînt adevărate, atunci q este adevărată. Însă p e adevărată din ipoteză, iar $p \to q$ este $\neg p \vee q$, adevărată căci $\neg p$ este adevărată.

Independenţa axiomelor: nici o axiomă nu este o consecinţă a celorlalte. O teorie în care axiomele nu sînt independente nu este însă lipsită de interes (poate fi, cel mult, acuzată de redundanţă).

Problemele stabilirii consistenţei şi independenţei unui sistem axiomatic sînt dificile şi profunde.

Strîns legată de problema consistenţei este *modelarea* unui sistem axiomatic. Se numeşte *model* al unei teorii axiomatice o structură de obiecte care satisfac axiomele teoriei. Se pot da exemple numeroase: un model al axiomelor geometriei plane este $\mathbb{R}\times\mathbb{R}$, un model pentru axiomele inelului este $(\mathbb{Z}, +, \cdot)$ etc. Are loc următorul rezultat: *o teorie axiomatică este consistentă dacă şi numai dacă are un model*.

Se observă că, în exemplele de mai sus, modelele teoriilor sînt obiecte construite în cadrul teoriei (axiomatice) a mulţimilor (care este mai largă decît teoriile respective). O teoremă a lui Gödel afirmă, într-o exprimare neriguroasă, că un model pentru o teorie axiomatică poate fi construit doar într-o teorie mai largă. Aşadar, un eventual model pentru ZF (care i-ar demonstra consistenţa) nu ar putea fi construit decît într-o teorie mai largă. Însă ZF este suficient de cuprinzătoare pentru a putea servi drept fundament al întregii matematici; pe de altă parte, verificarea consistenţei unei ipotetice teorii mai largi revine la construcţia unei teorii şi mai largi ş.a.m.d. Se vede că această cale nu conduce la o demonstraţie a consistenţei teoriei ZF. Se poate doar presupune că teoria ZF nu conduce la apariţia de contradicţii (de fapt, am văzut că a fost creată tocmai pentru a elimina contradicţiile apărute în teoria naivă a mulţimilor). În acest sens, este grăitor următorul citat din MANIN [1977], p. 102:

> Problema consistenţei formale a axiomelor Zermelo-Fraenkel trebuie să rămînă o chestiune de credinţă, cu excepţia cazului cînd o eventuală inconsistenţă formală este demonstrată. Pînă acum toate demonstraţiile bazate pe aceste axiome nu au dus niciodată la o contradicţie; dimpotrivă, au deschis în faţa noastră bogata lume a matematicilor clasice şi moderne. Această lume are o anumită realitate şi o viaţă proprii, care depind în mică măsură de formalismele alese pentru a le descrie. O descoperire a unei contradicţii în oricare din diversele formalisme, chiar dacă ar apărea, ar servi doar la clarificarea, rafinarea şi poate reconstrucţia unor anumite idei, dar nu ar conduce la falimentul lor, cum s-a întîmplat de mai multe ori în trecut.

Independenţa axiomelor are şi ea legătură cu consistenţa. Să exemplificăm aceasta pe cazul unei noi axiome, *axioma fundării*.

Axioma fundării (AF)**.** *Orice mulțime nevidă conține un element de care este disjunctă:*

$$(\forall a)[a \neq \varnothing \rightarrow (\exists b)(b \in a \wedge b \cap a = \varnothing)].$$

Acest enunț implică: *Nici o mulțime nu este element al ei însăşi*. Într-adevăr, dacă avem o mulțime x astfel încît $x \in x$, atunci $\{x\}$ contrazice axioma fundării: singurul element al lui $\{x\}$ este x şi avem $x \cap x$ nevidă, căci conține pe x. Mai mult, nu există „lanțuri de mulțimi" de forma $x_0 \in x_1 \in x_2 \in \ldots \in x_n \in x_0$. Dacă ar exista un asemenea lanț, atunci mulțimea $\{x_0, x_1, \ldots, x_n\}$ contrazice AF (de ce?). La fel, nu poate exista un şir $(x_n)_{n \in \omega}$ astfel încît $x_{n+1} \in x_n$, $\forall n \in \omega$. AF îşi datorează numele faptului că, pentru orice mulțime x, orice lanț de forma $x \ni x_0 \ni x_1 \ni \ldots \ni x_n \ni \ldots$ este finit şi se termină cu $\varnothing$: $\exists n$ astfel încît $x \ni x_0 \ni x_1 \ni \ldots \ni x_n \ni \varnothing$: orice şir descrescător (față de relația $\in$) este finit şi *„fundat"* pe $\varnothing$.[21]

S-a demonstrat că, dacă acceptăm că ZF este consistentă, atunci ZF + AF (sistemul ZF la care se adaugă AF) nu conduce la contradicții. Această probare a *consistenței relative* a AF s-a realizat prin construirea unui model (în cadrul ZF) care satisface ZF + AF. În plus, s-a construit un alt model (tot în cadrul ZF) care satisface ZF şi *negația AF*. Din aceste două rezultate se vede că AF este independentă de ZF (nu poate fi dedusă din axiomele ZF).

Un alt rezultat în această direcție este demonstrarea *independenței axiomei infinității față de restul axiomelor ZF*, printr-un procedeu principial asemănător cu cel de mai sus.

Axioma alegerii (AC)[22] este o nouă axiomă care joacă un rol deosebit în matematică, datorită faptului că, pe de o parte, are un enunț aparent „evident"; pe de altă parte, are un caracter neconstructiv care i-a atras multe critici. Există multe enunțuri echivalente cu această axiomă. În formularea lui Zermelo, AC se enunță:

Pentru orice mulțime A în care elementele sînt disjuncte două cîte două[23]*, există o mulțime care conține exact un element din fiecare mulțime nevidă din A* :

$$(\forall A)[(\forall x)(\forall y)(x \in A \wedge y \in A \wedge x \neq y) \rightarrow x \cap y = \varnothing] \rightarrow$$
$$(\exists c)[(\forall x)(x \in A \wedge x \neq \varnothing) \rightarrow (\exists z)(c \cap x = \{z\}].$$

Altfel spus, putem „alege" cîte un element din fiecare mulțime nevidă din A şi forma cu ele o nouă mulțime. Controversele privind această axiomă provin şi din faptul că se postulează existența unei astfel de mulțimi şi implicit a unui „procedeu de alegere" a unui element dintr-o mulțime nevidă. În 1963 s-a demonstrat că AC nu poate fi dedusă din ZF. În majoritatea matematicilor contemporane, AC este acceptată alături de ZF, în sistemul numit ZFC.

Există numeroase enunțuri echivalente cu Axioma Alegerii. Iată cîteva:

---

[21] Astfel, întregul univers descris de ZF şi AF este "creat" pornind de la $\varnothing$ (universul "von Neumann", vezi MANIN [1977], p. 95-102).

[22] Acronimul expresiei Axiom of Choice.

[23] Reamintim că elementele lui A sînt tot mulțimi.

Principiul bunei ordonări (Zermelo 1904). *Orice mulţime nevidă A poate fi bine ordonată* (*există o relaţie de bună ordine pe A*).

Produsul cartezian al unei familii de mulţimi nevide este nevid.

Pentru orice mulţime a, există o funcţie de alegere $f : a \to \bigcup a$ (adică f are proprietatea că, $\forall x \in a, x \neq \varnothing \to f(x) \in x$). [24]

Pentru orice funcţie surjectivă $\varphi : E \to F$ *există* $\psi : F \to E$ *astfel încît* $\varphi\psi = id_F$.

Lema lui Zorn. *Fie* $(A, \leq)$ *o mulţime ordonată nevidă în care orice submulţime total ordonată este majorată* (*mulţime „inductiv ordonată”*). *Atunci A conţine un element maximal.*

Lema lui Zorn este folosită în algebră în demonstrarea unor teoreme importante: existenţa unei baze într-un spaţiu vectorial oarecare, existenţa idealelor maximale într-un inel, existenţa închiderii algebrice a unui corp comutativ.

În continuare prezentăm cîteva noţiuni de *teoria cardinalilor*. Pentru o tratare mai în detaliu, vezi MIRON, NĂSTĂSESCU [1974], SCORPAN.

5.28 Definiţie. Fie A şi B două mulţimi. Spunem că A şi B sînt *echipotente* (sau că sînt *cardinal echivalente*, sau că *au acelaşi cardinal*) dacă există o bijecţie $f : A \to B$. Scriem atunci $A \sim B$ sau $|A| = |B|$.

Pentru orice mulţimi A, B, C, au loc:

a) $A \sim A$ (reflexivitate);

b) Dacă $A \sim B$, atunci $B \sim A$ (simetrie);

c) Dacă $A \sim B$ şi $B \sim C$, atunci $A \sim C$ (tranzitivitate).

Astfel, putem spune că relaţia de echipotenţă " ~ " este o relaţie de echivalenţă pe clasa mulţimilor. Clasa[25] tuturor mulţimilor echipotente cu o mulţime dată A se numeşte *cardinalul mulţimii A* şi se notează card A sau $|A|$. Spunem că A este o mulţime *finită* cu n elemente ($n \in \mathbb{N}$) dacă $A \sim \{1, \dots, n\}$ şi atunci notăm $|A| = |\{1, \dots, n\}| =: n$. O mulţime care nu este finită se numeşte *infinită*. Se poate demonstra că: *mulţimea A este infinită* $\Leftrightarrow$ *există o funcţie injectivă* $\varphi : A \to A$ *care nu este surjectivă* $\Leftrightarrow$ *există o funcţie injectivă* $\psi : \mathbb{N} \to A$.

Dacă $|A| = |\mathbb{N}|$, spunem că A este o mulţime *numărabilă*.

Se introduce o *relaţie de ordine* între cardinali: spunem că $|A| \leq |B|$ dacă există o funcţie injectivă $\varphi : A \to B$. Definiţia este corectă: dacă $A \sim A'$, $B \sim B'$ şi există o funcţie injectivă $\varphi : A \to B$, atunci există o există o funcţie injectivă $\varphi' : A' \to B'$ (demonstraţi!).

Se verifică imediat că, pentru orice mulţimi A, B, C are loc:

a) $|A| \leq |A|$ (*reflexivitate*);

b) $|A| \leq |B|$ şi $|B| \leq |C|$ implică $|A| \leq |C|$ (*tranzitivitate*);

---

[24] Altfel spus, funcţia f "alege" cîte un element $f(x)$ din fiecare mulţime nevidă $x \in a$.

[25] Nu putem vorbi de "*mulţimea* tuturor mulţimilor echipotente cu A".

Are loc următoarea teoremă importantă, care arată că $\leq$ este şi *antisimetrică* (deci are într-adevăr aceleaşi proprietăți ca o relație de ordine).

5.29 Teoremă. (Cantor-Schröder-Bernstein) *Fie A şi B două mulțimi. Dacă* $|A| \leq |B|$ *şi* $|B| \leq |A|$, *atunci* $|A| = |B|$.

Demonstrație. Idee: să găsim $D \subseteq A$ astfel încît $A \setminus D \subseteq \mathrm{Img}$ şi $\alpha : A \to B$, dată de:

$$\alpha(a) = \begin{cases} f(a) & \text{dacă } a \in D \\ g^{-1}(a) & \text{dacă } a \notin D \end{cases}$$

să fie o bijecție (faceți un desen!). Trebuie să avem atunci $A \setminus D = g(B \setminus f(D))$, adică $D = A \setminus g(B \setminus f(D))$.

Pentru a găsi D ca mai sus, definim $\varphi : \mathcal{P}(A) \to \mathcal{P}(A)$, $\varphi(E) := A \setminus g(B \setminus f(E))$, $\forall E \in \mathcal{P}(A)$. Noi căutăm un D cu $\varphi(D) = D$.

Se arată uşor că *φ este crescătoare*: dacă $E \subseteq F$, atunci $\varphi(E) \subseteq \varphi(F)$.

Definim $M := \{E \subseteq A \mid E \subseteq \varphi(E)\}$. Evident, M este nevidă căci, de exemplu, $\varnothing \in M$.

Fie $D := \bigcup\{E \mid E \in M\}$. Să arătăm că $\varphi(D) = D$. Avem $\varphi(D) = \varphi(\bigcup\{E \mid E \in M\}) = \bigcup\{\varphi(E) \mid E \in M\} \supseteq \bigcup\{E \mid E \in M\} = D$. Deci $D \subseteq \varphi(D)$. Aplicînd φ acestei incluziuni, obținem $\varphi(D) \subseteq \varphi(\varphi(D))$ adică $\varphi(D) \in M$. De aici, $D = \bigcup\{E \mid E \in M\} \supseteq \varphi(D)$. Astfel, $\varphi(D) = D$. Lăsăm cititorului verificarea faptului că α este bijecție. □

Relația de ordine $\leq$ este şi *totală* (demonstrația face apel la Axioma Alegerii):

5.30 Teoremă. *Oricare ar fi două mulțimi A, B, are loc* $|A| \leq |B|$ *sau* $|B| \leq |A|$. □

Această ultimă proprietate este echivalentă cu Axioma Alegerii.

Exerciții

1. Fie A, B mulțimi. Scrieți o expresie a limbajului formal care să semnifice că:

a) Mulțimea A nu este inclusă în mulțimea B.

b) $A \neq B$ (folosiți doar relația de apartenență).

b) Dacă $f : A \to B$ este o funcție, iar $C, D \subseteq A$, scrieți că $f(C) = f(D)$.

2. Demonstrați că axioma infinității este echivalentă cu enunțul: *Există un ordinal infinit.*

3. Demonstrați că clasa ordinalelor *On* nu este mulțime („paradoxul Burali-Forti”).

4. Demonstrați că reuniunea unei mulțimi A de ordinale este un ordinal şi este marginea superioară a lui A în *On*.

5. Un ordinal se numeşte *ordinal limită* dacă nu are un predecesor. Arătați că ω este cel mai mic ordinal limită şi că axioma infinității este echivalentă cu afirmația: *Există un ordinal limită.* Care este succesorul lui ω?

6. Arătaţi că ordinalul α este ordinal limită dacă şi numai dacă $\alpha = \sup \{\beta \mid \beta \in \alpha\}$ (margine superioară în *On*).

7. Inducţia transfinită (pe clasa ordinalelor *On*) se face adesea distingînd cazul ordinalelor limită. Mai precis, demonstraţi că dacă o expresie $P(x)$ are proprietăţile:

a) $P(\varnothing)$ adevărată;

b) $\forall \alpha\, [(On(\alpha) \wedge P(\alpha)) \rightarrow P(\alpha + 1)]$;

c) Pentru orice ordinal limită λ, dacă $P(\beta)$ adevărată, $\forall \beta < \lambda$, atunci $P(\lambda)$ adevărată,

atunci $P(\alpha)$ adevărată pentru orice ordinal α.

8. Axioma infinităţii face referire la mulţimea vidă $\varnothing$, a cărei existenţă rezultă din existenţa măcar a unei mulţimi. Dar acest lucru este asigurat de axioma infinităţii. Cum se poate ieşi din acest (aparent) cerc vicios?

9. Arătaţi că, pentru orice mulţime A, are loc $|\mathcal{P}(A)| > |A|$.

10. (Reprezentarea unui număr în baza b) Fie b un număr natural nenul fixat (numit *bază de numeraţie*). Demonstraţi că, $\forall a \in \mathbb{N}$, există şi sînt unice $n \in \mathbb{N}^*$ şi $c_0, \ldots, c_{n-1} \in \{0, 1, \ldots, b-1\}$, astfel încît

$$a = c_{n-1}b^{n-1} + \ldots + c_1 b + c_0 \qquad (R)$$

În cazul în care are loc egalitatea (R) de mai sus, se mai scrie $a = \overline{c_{n-1}\ldots c_1 c_0}$, scriere numită *reprezentarea lui a în baza b*. Numerele naturale 0, 1, …, $b - 1$ se numesc *cifre*[26] *în baza b* (pentru scrierea concretă se dau b simboluri care reprezintă aceste cifre şi nu se foloseşte bara superioară, scrisă aici pentru a evita confuzia cu produsul $c_{n-1}\ldots c_1 c_0$). Uneori, în notaţie, se mai specifică baza b, ca indice. De exemplu, $105_7 = 54_{10}$. (Ind. Din teorema împărţirii cu rest aplicată lui a şi b, $\exists!\ q, r \in \mathbb{N}$ astfel încît $a = bq + r$. Se pune $c_0 = r$ şi se repetă procedeul pentru q – sau, mai riguros, se aplică o inducţie după a. Pentru unicitate, se observă că c_0 este restul împărţirii lui a la b şi se aplică o inducţie după cel mai mic număr de cifre din ipoteticele reprezentări ale lui a în baza b).

11. Reprezentaţi în baza 10 numerele 1011_2, 1212_3. Scrieţi în bazele 2, 7, 16, numerele 129_{10}, 1152_{10}.

---

[26] A se remarca distincţia între *număr* şi *cifră* (într-o bază fixată). De exemplu, cifrele în baza 16 (sistem *hexadecimal*) sînt 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, unde A reprezintă pe 10 (scris în baza zece), B pe 11, …

II. Mulțimi factor şi construcții de structuri numerice fundamentale

Presupunînd cunoscută mulțimea $\mathbb{N}$ a numerelor naturale, înzestrat cu operațiile de adunare şi înmulțire (cu proprietățile cunoscute) şi cu structura sa de ordine uzuală ($\mathbb{N}$ este o mulțime *bine ordonată*), se pune problema *construirii celorlalte structuri numerice de bază*: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, la care putem adăuga inelele de clase de resturi $\mathbb{Z}_n$.

Se impune un comentariu privind noțiunea de „număr”. În multe cărți se pun întrebări (probleme) de genul „ce este *numărul* (eventual rațional sau real sau complex)”, urmînd ca autorul să dea un răspuns de natură filozofică sau matematică. Noțiunea de *număr* (privit ca element individual, izolat) nu are o semnificație deosebită în matematică, mult mai importantă fiind cea de *structură pe o mulțime numerică*. Astfel, de pildă mulțimea $\mathbb{R}$ a numerelor reale este importantă prin *structurile* cu care este înzestrată: structura *algebrică* de corp comutativ, cea de *ordine* (este total ordonată şi orice submulțime majorată are supremum), cea *topologică* derivată din acestea (este spațiu metric complet); un număr real, luat ca element individual al lui $\mathbb{R}$, nu poate fi pus nicidecum în legătură cu astfel de proprietăți. Insistăm asupra acestei distincții pentru că o conştientizare a ei îşi poate pune amprenta şi asupra stilului de predare a acestor concepte fundamentale.

II.1. Relații de echivalență şi mulțimi factor

Relațiile de echivalență sînt un instrument esențial în matematică, mai ales în problemele de *construcții* de obiecte (structuri) noi. Vom descrie un procedeu general, *construcția mulțimii factor (cît) în raport cu o relație de echivalență*, care, aplicat în diverse cazuri particulare, duce la construcții importante. Trebuie subliniat că mulțimea factor obținută se înzestrează cu o structură care este de obicei legată de structura mulțimii inițiale (ceea ce presupune o *compatibilitate între relația de echivalență şi structura inițială*). Această metodă permite construcția unor structuri matematice importante: $\mathbb{Z}$ (construit ca mulțime factor a lui $\mathbb{N} \times \mathbb{N}$), $\mathbb{Q}$ (mulțime factor a lui $\mathbb{Z} \times \mathbb{Z}^*$; acelaşi procedeu dă în general inele şi corpuri de fracții), $\mathbb{R}$ (mulțime factor a mulțimii şirurilor Cauchy de numere raționale), $\mathbb{C}$ (mulțime factor

a inelului de polinoame $\mathbb{R}[X]$). Remarcăm că majoritatea construcțiilor în matematică sînt mulțimi factor în raport cu o anumită relație de echivalență: produsul tensorial a două module, grupul liber pe o mulțime, spațiile proiective din geometrie, spațiile L^p din analiză, … şi lista este departe de a fi completă.

Fie A o mulțime şi ρ o relație de echivalență pe A. Mulțimea

$$\{x \in A \mid x\rho a\}$$

poartă numele de *clasa de echivalență* a elementului a relativ la relația ρ şi se notează cu $\hat{a}$. Se folosesc adesea multe alte notații, depinzînd de cazul particular ales şi de dorința de a include sau nu relația ρ în notație. De exemplu, clasa lui a se mai notează C_a, $\bar{a}$, $\hat{a}_\rho$, $[a]_\rho$ etc.

Dacă pentru elementele a şi b are loc $a\rho b$, mai spunem că a şi b sînt *echivalente modulo* ρ.

1.1 Definiție. Mulțimea claselor de echivalență în raport cu relația ρ se numeşte *mulțimea cît* (sau *factor*) a lui A în raport cu ρ şi se notează cu A/ρ. Deci $A/\rho := \{\hat{a} \mid a \in A\}$.

1.2 Propoziție. *Fie ρ o relație de echivalență pe A. Atunci:*

a) $\forall a \in A$ are loc $a \in \hat{a}$ (deci $\hat{a}$ este nevidă).

b) $\forall a, b \in A$, avem: $\hat{a} = \hat{b} \Leftrightarrow a\rho b$.

c) $\forall a, b \in A$, are loc fie $\hat{a} = \hat{b}$, fie $\hat{a} \cap \hat{b} = \varnothing$.

d) $\bigcup_{a \in A} \hat{a} = A$. □

O mulțime P de submulțimi nevide ale lui A, disjuncte două cîte două, a căror reuniune este A, este numită *partiție* a lui A. Mai precis, avem:

a) $\forall B\ (B \in P) \rightarrow B \neq \varnothing$;

b) $\forall B\ [(B \in P) \wedge (C \in P) \wedge (B \neq C)] \rightarrow (B \cap C = \varnothing)$;

c) $\bigcup\{B \mid B \in P\} = A$.

Propoziția anterioară nu spune altceva decît că *mulțimea factor a lui A în raport cu o relație de echivalență este o partiție a lui A.* Reciproc, orice partiție poate fi obținută dintr-o relație de echivalență:

1.3 Propoziție. *Fie P o partiție a mulțimii A. Atunci relația ρ definită prin:*

$$\forall a, b \in A,\ a\rho b \Leftrightarrow \exists B \in P \text{ astfel încît } a \in P \text{ şi } b \in P$$

este o relație de echivalență pe A şi P este chiar mulțimea cît A/ρ. □

În aplicații, mulțimea inițială are de obicei o *structură* (algebrică, topologică, de ordine,…), iar relația de echivalență este *compatibilă* cu structura dată (sensul precis al acestei compatibilități fiind definit în fiecare caz în parte; în general, definiția este „naturală”). Atunci mulțimea factor obținută va moşteni o structură de acelaşi tip ca mulțimea inițială. Vom prezenta exemple de aplicare în algebră a acestei construcții fundamentale (trecerea de la o mulțime la mulțimea factor în raport cu o relație de echivalență) în paragrafele următoare.

Un concept important este cel de *sistem de reprezentanți.*

1.4 Definiție. Fie ρ o relație de echivalență pe mulțimea A. Spunem că submulțimea $S \subseteq A$ este un *sistem de reprezentanți*[27] *pentru clasele de echivalență* (*modulo* ρ) dacă orice element din A este echivalent modulo ρ cu exact un element din S. Intuitiv, un sistem de reprezentanți se obține „alegînd" din fiecare clasă de echivalență cîte un element („reprezentantul" clasei respective). Astfel S este sistem de reprezentanți dacă şi numai dacă:

$$(\forall a \in A)(\exists s \in S)(a\rho s) \wedge (\forall s, t \in S)(\ (s\rho t) \rightarrow s = t).$$

1.5 Exerciții. a) Fie relația de echivalență definită pe $\mathbb{R}^2$ (identificat cu un plan în care s-a ales un sistem de coordonate Oxy): $(x, y) \sim (z, t) \Leftrightarrow x = z$. Clasele de echivalență sînt dreptele paralele cu Oy. Un sistem de reprezentanți este (de exemplu) $\{(x,0) \mid x \in \mathbb{R}\}$. Mulțimea factor $\mathbb{R}^2/\sim$ este în bijecție cu $\mathbb{R}$. Cum se poate defini o relație de echivalență pe $\mathbb{R}^2$ astfel încît clasele de echivalență să fie dreptele paralele cu o dreaptă fixată ce trece prin origine, de ecuație $y = \alpha x$?

b) Puteți defini o relație de echivalență pe $\mathbb{R}^2$ astfel încît clasele de echivalență să fie cercurile concentrice cu centrul în origine? Dar pătrate centrate în origine, cu laturile paralele cu axele? Dar pătrate centrate în origine, cu laturile paralele cu bisectoarele sistemului de axe?

c) Pe $\mathbb{R}$ definim relația de „congruență modulo $\mathbb{Z}$": pentru $x, y \in \mathbb{R}$, spunem că $x \equiv y \pmod{\mathbb{Z}}$ dacă $x - y \in \mathbb{Z}$. Un sistem de reprezentanți este dat de intervalul $[0, 1)$. Acesta este un caz particular de grup factor (în cazul nostru $\mathbb{R}/\mathbb{Z}$).

d) *Închiderea tranzitivă a unei relații.* Fie ρ o relație pe mulțimea A. Definim o nouă relație τ_ρ pe A, astfel: $\forall a, b \in A$, $a\tau_\rho b \Leftrightarrow \exists n \in \mathbb{N}$ şi $x_1, \ldots, x_n \in A$ astfel încît $a = x_1$, $b = x_n$ şi $x_i\,\rho\,x_{i+1}$, $i = 1,\ldots, n-1$. Atunci τ_ρ este o relație *tranzitivă* pe A. Mai mult, τ_ρ este cea mai mică (în sensul incluziunii) relație tranzitivă pe A care include relația ρ.

II.2. Inelul numerelor întregi

Necesitatea considerării numerelor negative apare din considerente practice, binecunoscute cititorilor (pentru a modela situații precum: temperaturi negative, datorii în conturi bancare etc.), dar şi din considerente matematice: diferența a două numere naturale nu este întotdeauna definită ca un număr natural. Formulat altfel, nu pentru orice $a, b \in \mathbb{N}$ ecuația $x + a = b$ are soluții $x \in \mathbb{N}$.

[27] O denumire mai corectă, dar mai greu de manipulat, este *sistem complet şi independent de reprezentanți.*

De aici apare şi ideea de a concepe un „număr întreg negativ” ca o *diferenţă* de numere naturale. Bineînţeles, pentru o „diferenţă” dată există mai multe (chiar o infinitate de) perechi de numere naturale care au aceeaşi diferenţă: de exemplu perechile (0, 1), (1, 2), (2, 3), … au aceeaşi diferenţă (numărul întreg -1). Ar trebui deci să vedem un număr întreg ca pe o pereche de numere naturale (de forma (a, b)), cu convenţia că „se consideră egale” două perechi (a, b) şi (c, d) dacă $a - b = c - d$. Cum scăderea nu este definită pentru orice pereche de numere naturale, rescriem această condiţie sub forma $a + d = b + c$. Exprimăm riguros aceste consideraţii euristice:

Pe mulţimea $\mathbb{N} \times \mathbb{N}$ se consideră relaţia $\sim$, definită prin:

$$\forall (a, b), (c, d) \in \mathbb{N} \times \mathbb{N} : (a, b) \sim (c, d) \Leftrightarrow a + d = b + c$$

Se demonstrează (verificaţi!) că aceasta este o relaţie de echivalenţă. O clasă de echivalenţă în raport cu această relaţie o numim *număr întreg*, iar mulţimea factor $\mathbb{N} \times \mathbb{N}/\sim$ se numeşte *mulţimea numerelor întregi* şi se notează cu $\mathbb{Z}$.

Notaţia $\mathbb{Z}$ provine de la cuvîntul german *zahl* (pronunţat *ţal*, cu un *a* lung), care înseamnă *număr*. A se observa grafia ($\mathbb{Z}$ şi nu Z), litera $\mathbb{Z}$ scrisă astfel fiind rezervată exclusiv notării mulţimii numerelor întregi (după cum $\mathbb{N}$ este folosită exclusiv pentru mulţimea numerelor naturale).

Nu ne putem opri aici cu construcţia. Trebuie arătat că obiectul pe care l-am construit (riguros) satisface toate proprietăţile pe care ne-am aştepta să le aibă mulţimea numerelor întregi: „include” mulţimea $\mathbb{N}$, orice număr întreg este sau număr natural, sau opusul unui număr natural, este definită o adunare şi o înmulţire în raport cu care este inel, este o mulţime total ordonată, iar ordinea este compatibilă cu adunarea şi înmulţirea.

Mai întîi să determinăm un sistem de reprezentanţi. Mulţimea

$$Z := \{(a, 0) \mid a \in \mathbb{N}\} \cup \{(0, a) \mid a \in \mathbb{N}^*\}$$

este sistem de reprezentanţi: dacă $a \geq b$, atunci $(a, b) \sim (a - b, 0)$, iar dacă $a < b$, atunci $(a, b) \sim (0, b - a)$. Vom *identifica* numărul natural a cu clasa de echivalenţă a lui $(a, 0)$ (lucru permis de faptul că aplicaţia care duce a în $(a, 0)$ este injectivă de la $\mathbb{N}$ la $\mathbb{N} \times \mathbb{N}/\sim$, demonstraţi!) şi vom nota cu $-a$ clasa de echivalenţă a lui $(0, a)$. Ce mai trebuie verificat pentru a demonstra că Z, definit mai sus, este sistem de reprezentanţi?

Cu aceste identificări, putem scrie:

$$\mathbb{Z} = \{a \mid a \in \mathbb{N}\} \cup \{-a \mid a \in \mathbb{N}^*\}.$$

Să definim *operaţiile de adunare şi înmulţire* pe $\mathbb{Z}$ (pornind de la cele de pe $\mathbb{N}$). Pentru aceasta, se definesc operaţii pe clasele de echivalenţă din $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$, folosind reprezentanţi oarecare, urmînd să se demonstreze că nu depind de reprezentanţi şi deci sînt corect definite. De exemplu, notînd cu $\overline{(a, b)} \in \mathbb{N} \times \mathbb{N}/\sim$ clasa lui $(a, b) \in \mathbb{N} \times \mathbb{N}$, definim

$$\overline{(a, b)} + \overline{(c, d)} := \overline{(a + c, b + d)}.$$

Bineînțeles, $a + c$ semnifică suma în $\mathbb{N}$ a numerelor naturale a şi c. Operația este *corect definită*.[28] Aceasta înseamnă că, $\forall(a, b)$, $(c, d) \in \mathbb{N} \times \mathbb{N}$ cu $(a, b) \sim (a', b')$ şi $(c, d) \sim (c', d')$, atunci $(a + c, b + d) \sim (a' + c', b' + d')$. Verificarea este uşoară şi constă în aplicarea definițiilor relației de echivalență şi a operației $+$.

Invităm cititorul să definească înmulțirea, să demonstreze corectitudinea definiției şi proprietățile uzuale ale operațiilor, care conferă lui $\mathbb{Z}$ structură de *inel comutativ şi unitar, fără divizori ai lui* 0 (se mai spune că $\mathbb{Z}$ este *inel integru* sau *domeniu de integritate*).

Relația de ordine pe $\mathbb{Z}$: fie $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$. Spunem că $\overline{(a, b)} \le \overline{(c, d)}$ dacă şi numai dacă $a + d \ge b + c$ în $\mathbb{N}$ (de ce am definit astfel?). Demonstrați corectitudinea definiției şi faptul că se obține o *relație de ordine totală* pe $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$.

Se mai pot defini operațiile pe $\mathbb{Z}$ (respectiv relația de ordine pe $\mathbb{Z}$) folosind sistemul de reprezentanți Z de mai sus şi operațiile din $\mathbb{N}$ (cum?). Ce avantaje şi dezavantaje au cele două abordări?

O funcție deosebit de importantă este funcția *valoare absolută* (sau *modul*) $|\ | : \mathbb{Z} \to \mathbb{Z}$,

$$|x| = \begin{cases} x & \text{dacă } x \ge 0 \\ -x & \text{dacă } x < 0 \end{cases}$$

Importanța acestei funcții apare în legătură cu faptul că $\mathbb{Z}$ este *inel euclidian*, adică are loc:

2.1 Teoremă. (Teorema împărțirii cu rest în $\mathbb{Z}$) *Pentru orice numere întregi a, b, cu* $b \ne 0$*, există* $q, r \in \mathbb{N}$*, astfel încît* $a = bq + r$*, cu* $r = 0$ *sau* $|r| < |b|$ (*q se numeşte* cît, *iar r* rest al împărțirii lui *a* la *b*). *Dacă se impune şi* $r > 0$*, q şi r sînt unic determinate cu aceste proprietăți.* ☐

II.3. Corpul numerelor raționale. Inele şi corpuri de fracții

În gimnaziu, se introduc mai întîi doar numerele raționale *pozitive*, din motive didactice. Această distincție oarecum artificială nu îşi are locul aici. Din punct de vedere algebric, construcția lui $\mathbb{Q}$ pornind de la $\mathbb{Z}$ este principial aceeaşi cu construcția *corpului de fracții al unui inel integru oarecare R*.

Introducerea lui $\mathbb{Q}$ este motivată, printre altele, de imposibilitatea efectuării unor împărțiri în $\mathbb{Z}$. De exemplu, nu este definit rezultatul (cîtul) împărțirii lui 3 la 2; altfel spus, ecuația $3x = 2$ nu are soluții în $\mathbb{Z}$. Mai general, dacă $b, a \in \mathbb{Z}$ şi a nu divide b, ecuația $bx = a$ nu are

---

[28] Subliniem că necesitatea demonstrării corectitudinii definiției apare tot timpul cînd se dau definiții pe o mulțime factor, folosind reprezentanți oarecare ai claselor.

soluții în $\mathbb{Z}$. Apare ideea (similară cu aceea de la construcția precedentă a lui $\mathbb{Z}$) de a introduce o nouă mulțime de numere (numerele *raționale*) ca fiind „toate cîturile posibile de numere întregi”. De exemplu, cîtul împărțirii lui 3 la 2 va fi „numărul rațional” („fracția”) $3/2$. Deoarece acelaşi cît este dat şi de împărțirea lui 6 la 4 (sau a lui 9 la 6 etc.), este necesar să precizăm *cînd două fracții a/b şi c/d sînt egale*. Aceasta revine la *a defini o relație de echivalență* pe mulțimea perechilor de forma (a, b), cu $a, b \in \mathbb{Z}$, $b \neq 0$ (o fracție va fi o clasă de echivalență de perechi). Relația de echivalență este definită de

$$\forall\ (a, b), (c, d) \in \mathbb{Z}\times\mathbb{Z}^*,\quad (a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Cititorul poate demonstra uşor că este vorba într-adevăr de o relație de echivalență.

O clasă de echivalență (un element al mulțimii $\mathbb{Z}\times\mathbb{Z}^*/\sim$) este notată cu a/b sau $\dfrac{a}{b}$ şi este numit(ă) *fracție*; a este *numărătorul*, iar b este *numitorul* fracției a/b. Mulțimea fracțiilor (mulțimea cît $\mathbb{Z}\times\mathbb{Z}^*/\sim$) se notează prin tradiție cu $\mathbb{Q}$ (de la inițiala cuvîntului *quotient*, care înseamnă *cît* în engleză şi în franceză). Mulțimea $\mathbb{Z}$ se poate identifica cu o parte a lui $\mathbb{Q}$: numărul întreg a se identifică cu fracția $\dfrac{a}{1}$. Pe $\mathbb{Q}$ se introduc operațiile de adunare şi înmulțire, inspirate de regulile cunoscute din gimnaziu (aducerea la acelaşi numitor etc.):

$$\forall\ a/b, c/d \in \mathbb{Q},\ \ \frac{a}{b}+\frac{c}{d} := \frac{ad+bc}{bd};\ \ \frac{a}{b}\cdot\frac{c}{d} := \frac{ac}{bd}$$

Ca şi la construcția lui $\mathbb{Z}$, trebuie arătat că *definițiile sînt corecte* (nu depind de alegerea reprezentanților fracțiilor) şi că $\mathbb{Q}$, înzestrat cu aceste operații, este *inel comutativ unitar* (elementul nul este fracția $0/1$, iar elementul unitate este fracția $1/1$). Mai mult, $\mathbb{Q}$ este *corp*: orice element nenul $\dfrac{a}{b}$ are invers față de înmulțire: $\left(\dfrac{a}{b}\right)^{-1} = \dfrac{b}{a}$.

Importanța construcției de mai sus depăşeşte cadrul elementar al construcției lui $\mathbb{Q}$; aceeaşi idee, cu modificări minore, se aplică la *construcția inelului de fracții al unui inel comutativ relativ la un sistem multiplicativ închis* al său, construcție fundamentală în toată matematica.

3.1 Definiție. Fie R un inel comutativ unitar. O submulțime nevidă S a lui R se numeşte *sistem multiplicativ închis* dacă $1 \in S$ şi, oricare ar fi $x, y \in S$, rezultă $xy \in S$.

3.2 Observație. Ideea care motivează introducerea noțiunii de mai sus este următoarea: se doreşte o construcție a unei mulțimi de fracții *cu numitori din S*. Cum produsul a doi numitori trebuie să fie tot un numitor, este naturală impunerea condiției ca S să fie parte stabilă la înmulțire. De asemenea, este naturală considerarea fracțiilor cu numitorul 1 (adică $1 \in S$). Exemple de sisteme multiplicative închise: $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ în $\mathbb{Z}$; $\mathbb{Z} \setminus 2\mathbb{Z}$ în $\mathbb{Z}$; $K[X] \setminus \{0\}$ în $K[X]$ (cu K un corp fixat şi $K[X]$ inelul polinoamelor cu coeficienți în K).

Fixăm un *inel comutativ unitar R şi un sistem multiplicativ închis S* al său. Ghidîndu-ne după echivalența binecunoscută $\frac{a}{s} = \frac{b}{t} \Leftrightarrow at = bs$, enunțăm următoarea:

3.3 Definiție. Pe mulțimea $R \times S$ se defineşte următoarea *relație*:

$$\forall\ (a, s), (b, t) \in R\times S, \text{ scriem } (a, s) \sim (b, t) \text{ dacă şi numai dacă } at = bs. \qquad (D)$$

Dacă $0 \notin S$ şi *S nu conține divizori ai lui zero* în R (un element nenul $x \in R$ se numeşte divizor al lui zero dacă $\exists y \in R$, $y \neq 0$, astfel încît $xy = 0$), atunci relația definită este *relație de echivalență* (Exercițiu!).

În cazul în care S poate conține divizori ai lui zero este necesară modificarea definiției (D) :

$$\forall\ (a, s), (b, t) \in R \times S, \quad (a, s) \sim (b, t) \Leftrightarrow \exists u \in S \text{ astfel încît } u(at - bs) = 0. \qquad (D')$$

Este clar că, dacă S nu conține divizori ai lui zero şi $0 \notin S$, (D) şi (D') coincid.

Arătăm că *D' este relație de echivalență*:

- *reflexivitatea:* $\forall(a, s) \in R \times S$, avem $(a, s) \sim (a, s)$ căci $\exists 1 \in S$ astfel încît $1(as - as) = 0$.

- *simetria:* dacă $(a, s) \sim (b, t)$, atunci $\exists u \in S$ astfel încît $u(at - bs) = 0$, deci $u(bs - at) = 0$, adică $(b, t) \sim (a, s)$.

- *tranzitivitatea:* fie $(a, s), (b, t), (c, u) \in R \times S$, astfel încît $(a, s) \sim (b, t)$ şi $(b, t) \sim (c, u)$. Din definiție, rezultă că $\exists x \in S$ astfel încît $x(at - bs) = 0$ şi $\exists y \in S$ astfel încît $y(bu - ct) = 0$. Vrem să obținem o relație de forma $z(au - cs) = 0$, pentru un $z \in S$. Înmulțind cu uy, respectiv sx, obținem:

$$uyxat - uyxbs = 0$$
$$sxybu - sxyct = 0$$

Adunînd membru cu membru şi observînd că $uyxbs = sxybu$, rezultă $uyxat - sxyct = 0$, adică $xyt(au - cs) = 0$. Cum $xyt \in S$ (sistem multiplicativ închis), aceasta înseamnă că $(a, s) \sim (c, u)$.

3.4 Definiție. Fie $(a, s) \in R \times S$. Clasa de echivalență a lui (a, s) în raport cu relația $\sim$ se notează cu $\frac{a}{s}$ sau a/s şi se numeşte *fracție* (de *numitor s* şi *numărător a*). Mulțimea $R \times S/\sim$ (mulțimea claselor de echivalență în raport cu relația $\sim$) se notează cu $S^{-1}R$. Deci

$$S^{-1}R := \{\ a/s \mid a \in R, s \in S\}.$$

Direct din definiție rezultă regula de „amplificare a fracțiilor” cu numitori din S:

$$\frac{a}{s} = \frac{ta}{ts},\ \forall s, t \in S, \forall a \in R.$$

Înzestrăm $S^{-1}R$ cu o structură de inel, inspirîndu-ne din regulile uzuale de adunare şi înmulțire a două fracții. Fie $(a, s), (b, t) \in R \times S$. Definim:

$$\frac{a}{s} + \frac{b}{t} := \frac{ta + sb}{st}$$
$$\frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}$$

3.5 Propoziție. *Operațiile* $+$ *şi* $\cdot$ *pe* $S^{-1}R$ *sînt bine definite şi înzestrează pe* $S^{-1}R$ *cu o structură de inel comutativ şi unitar. Elementele* 0 *şi* 1 *în* $S^{-1}R$ *sînt:*

$$0 = \frac{0}{1} = \frac{0}{s},\ \forall s \in S;$$

$$1 = \frac{1}{1} = \frac{s}{s},\ \forall s \in S.$$

Aplicația $\varphi : R \to S^{-1}R,\ \varphi(a) = a/1,\ \forall a \in R,$ *este un morfism unitar de inele, numit* morfismul canonic (*deci* $S^{-1}R$ *este o* R-algebră comutativă (*vezi definiția* **III.1.1**)).

Demonstrație. *Adunarea este corect definită*. Fie (a, s), (b, t), (a', s'), $(b', t') \in R \times S$, astfel încît $(a, s) \sim (a', s')$ şi $(b, t) \sim (b', t')$. Avem de arătat că $(ta + sb, st) \sim (t'a' + s'b', s't')$. Fie $u, v \in S$ astfel încît $u(s'a - sa') = 0$ şi $v(t'b - tb') = 0$. Înmulțim prima egalitate cu $tt'v$ şi a doua cu $ss'u$ şi le adunăm. Obținem

$$vu((ta + sb)s't' - (t'a' + s'b')st) = 0.$$

Restul verificărilor sînt lăsate cititorului. □

Observăm că orice $s \in S$ are imaginea prin φ *inversabilă* în $S^{-1}R$: $\varphi(s) = s/1$ are inversul $1/s$. Deci construcția efectuată rezolvă problema pusă la început: chiar dacă ecuația $sx = b$ nu are soluții în R (unde $s \in S$), în $S^{-1}R$ există soluția $x = \dfrac{b}{s}$. Această proprietate a inelului de fracții este foarte importantă (vezi 3.9 mai jos).

3.6 Observație. *a) Avem:* $x/1 = 0$ în $S^{-1}R \Leftrightarrow \exists s \in S$ *astfel încît* $sx = 0$. Acest fapt este imediat din definiție.

b) Morfismul φ *este injectiv* $\Leftrightarrow$ *S nu conține divizori ai lui* 0.

Într-adevăr, fie φ injectiv. Dacă, prin absurd, $s \in S$ este divizor al lui 0, atunci $\exists x \in R$, $x \neq 0$, astfel încît $xs = 0$. Atunci $\varphi(x) = x/1 = 0$ (căci $sx = 0$), contradicție cu injectivitatea lui φ. Reciproca e propusă ca exercițiu.

c) Dacă $0 \in S$, *atunci* $S^{-1}R$ *este inelul nul* (căci $a/s = 0/1$, $\forall a \in R$, $\forall s \in S$: $\exists 0 \in S$ astfel încît $0 \cdot a = 0$). De aceea, *în definiția sistemului multiplicativ închis se pune adesea condiția* $0 \notin S$.

3.7 Cazuri particulare importante. *Dacă R este inel integru şi* $S = R \setminus \{0\}$, *atunci* $S^{-1}R$ *este corp, numit* corpul total de fracții *al lui R şi notat uneori cu* $Q(R)$. Într-adevăr, orice fracție nenulă a/b $(a, b \in R, b \neq 0)$ are inversul b/a. În particular, $Q(\mathbb{Z}) = \mathbb{Q}$ (corpul de fracții al lui $\mathbb{Z}$ este $\mathbb{Q}$). Corpul de fracții al unui inel de polinoame $K[X]$ (unde K este corp) se notează cu $K(X)$ şi se numeşte corpul fracțiilor raționale cu coeficienți în K.

3.8 Teoremă. (Proprietatea de universalitate a inelului de fracții) *Fie R un inel unitar, comutativ şi S un sistem multiplicativ închis în R. Atunci* $S^{-1}R$ *este un inel comutativ unitar şi* $\varphi : R \to S^{-1}R$ *este un morfism unitar astfel încît* $\varphi(s)$ *este inversabil în S,* $\forall s \in S$. *Mai mult:*

Pentru orice inel comutativ unitar T şi orice morfism unitar $\gamma : R \to T$ *astfel încît* $\gamma(s)$ *este inversabil în T,* $\forall s \in S$*, există un unic morfism de inele* $g : S^{-1}R \to T$ *astfel încît* $\gamma = g\varphi$.

Demonstrație. Definim $g(a/s) = \gamma(a)(\gamma(s))^{-1}$, $\forall a \in R$, $\forall s \in S$. Lăsăm cititorului verificarea faptelor că g este corect definit, că este morfism şi că este unic astfel încît $\gamma = g\varphi$. □

În termeni de *R-algebre*, partea a doua a teoremei se formulează echivalent: pentru orice R-algebră comutativă T de morfism structural $\gamma : R \to T$, astfel încît $\gamma(s)$ este inversabil în T, $\forall s \in S$, există un unic morfism de R-algebre $g : S^{-1}R \to T$.

Teorema următoare exprimă faptul că proprietatea de universalitate a inelului de fracții determină inelul de fracții pînă la un (unic) izomorfism:

3.9 Teoremă. *Fie R un inel unitar, comutativ şi S un sistem multiplicativ închis în R. Presupunem că B este un inel comutativ unitar şi* $\beta : R \to B$ *este un morfism astfel încît:*

Pentru orice inel comutativ unitar T şi orice morfism unitar $\gamma : R \to T$ *astfel încît* $\gamma(s)$ *este inversabil în T,* $\forall s \in S$*, există un unic morfism de inele* $g : B \to T$ *astfel încît* $\gamma = g\beta$.

Atunci există un unic izomorfism unitar de inele $h : S^{-1}R \to B$ *astfel încît* $h\varphi = \beta$.

Demonstrație. Definim $g(a/s) = \gamma(a)(\gamma(s))^{-1}$, $\forall a \in R$, $\forall s \in S$. Lăsăm cititorului verificarea faptului că definiția lui g este corectă, că g este morfism şi că este unicul astfel încît $\gamma = g\varphi$. □

Un exemplu important, destul de general, de sistem multiplicativ închis şi de inel de fracții corespunzător este următorul:

3.10 Propoziție. *Fie P un ideal prim în inelul R. Atunci* $S := R \setminus P$ *este un sistem multiplicativ închis în R şi inelul de fracții* $S^{-1}R$ *are un unic ideal maximal* (*este inel* local).

Demonstrație. Condiția de ideal prim este: dacă $a, b \notin P$, atunci $ab \notin P$, ceea ce arată că S este sistem multiplicativ închis. Dacă $I \le R$, $I \cap S \ne \varnothing$, atunci $S^{-1}I = S^{-1}R$. Într-adevăr, dacă $s \in I \cap S$, atunci $s/1 \in S^{-1}I$ şi este inversabil, deci $S^{-1}I = R$. Aşadar, idealele proprii în $S^{-1}R$ sînt de forma $J = S^{-1}I$, cu $I \cap S = \varnothing$ ($\Leftrightarrow I \subseteq P$), adică $J \subseteq S^{-1}P$. Dar $S^{-1}P$ este ideal propriu: dacă $1/1 = p/s$, cu $p \in P$, $s \in S$, atunci $\exists u \in S$ astfel încît $u(s - p) = 0 \Rightarrow us \in P \Rightarrow u \in P$ sau $s \in P$, contradicție cu $S = R \setminus P$. Astfel, $S^{-1}P$ este unicul ideal maximal în $S^{-1}R$. □

Dacă $S = R \setminus P$, cu P ideal prim, inelul de fracții $S^{-1}R$ se notează de obicei prin R_P şi se numeşte *localizatul* în P al lui R. Avantajul acestei treceri este că se reduc multe probleme referitoare la idealul prim P din R la idealul maximal $S^{-1}P$ din localizatul $S^{-1}R$. De exemplu, dacă R este integru, atunci (0) este ideal prim şi $R_{(0)}$ este corpul de fracții al lui R.

Menționăm că se pot construi inele de fracții - în anumite condiții - şi în cazul inelelor necomutative (vezi de ex. NĂSTĂSESCU [1976]).

Revenim la corpul numerelor raționale $\mathbb{Q}$, care, în terminologia de mai sus, este *corpul total de fracții al lui* $\mathbb{Z}$. Rămîne să definim ordinea uzuală pe $\mathbb{Q}$.

3.11 Definiție. Fie a/b şi $c/d \in \mathbb{Q}$, unde $a, b, c, d \in \mathbb{Z}$, cu $b, d > 0$. Definim:

$$a/b \le c/d \Leftrightarrow ad \le bc.$$

Corectitudinea definiției este propusă ca exercițiu.

3.12 Definiție. Un corp comutativ $(K, +, \cdot)$ se numeşte *corp ordonat* dacă este înzestrat cu o relație de ordine totală " $\le$ " pe K astfel încît, $\forall a, b, c \in K$, au loc:

i) $a \le b \Rightarrow a + c \le b + c$;

ii) $a \le b$ şi $c \ge 0 \Rightarrow ac \le bc$.

$\mathbb{Q}$ este un corp ordonat față de relația de ordine uzuală; mai mult, orice relație de ordine pe $\mathbb{Q}$ în raport cu care acesta devine un corp ordonat coincide cu ordinea uzuală (vezi Exerciții). O funcție deosebit de importantă pentru un corp ordonat K este *valoarea absolută* (*modulul*) $|\ | : K \to K$, definit la fel ca valoarea absolută pe $\mathbb{Z}$:

$$|x| = \begin{cases} x & \text{dacă } x \ge 0 \\ -x & \text{dacă } x < 0 \end{cases}$$

Exerciții

1. Fie $\mathbb{Z}[X]$ inelul polinoamelor cu coeficienți în $\mathbb{Z}$. Atunci $Q(\mathbb{Z}[X])$ (corpul de fracții al lui $\mathbb{Z}[X]$) este izomorf cu *corpul fracțiilor raționale* $\mathbb{Q}(X) := Q(\mathbb{Q}[X])$.

2. Este adevărat că, dacă inelele integre R şi S au proprietatea $Q(R) \cong Q(S)$, rezultă că $R \cong S$?

3. Demonstrați că orice element din $\mathbb{Q}$ se poate scrie ca o fracție a/b, cu $a, b \in \mathbb{Z}$ şi $b > 0$.

4. Fie I un ideal în inelul R. Atunci $S^{-1}I := \{a/s \mid a \in I, s \in S\}$ este ideal în $S^{-1}R$. Mai mult, orice ideal din $S^{-1}R$ este de forma $S^{-1}I$, cu I ideal în R.

5. Demonstrați că relația de ordine uzuală pe $\mathbb{Q}$ (vezi def. II.3.11) este corect definită şi $\mathbb{Q}$ devine corp ordonat.

6. Fie $(K, +, \cdot, \le)$ un corp ordonat, cu element nul 0 şi element unitate 1. Atunci, $\forall a, b, c \in K$, au loc: a) $a \le b \Rightarrow -a \ge -b$; b) $0 < 1$; c) $0 < n\cdot 1$, $\forall n \in \mathbb{N}$; d) $0 < a$ şi $0 < b \Rightarrow 0 < ab$ şi $0 < a^{-1}$; e) $0 < a < b \Rightarrow 0 < b^{-1} < a^{-1}$.

În particular, car $K = 0$ (adică $n\cdot 1 \ne 0$, $\forall n \in \mathbb{N}^*$) şi există un unic morfism de corpuri $\varphi : \mathbb{Q} \to K$ (cf. proprietatea de universalitate II.3.8 aplicată funcției $n \mapsto n\cdot 1$ de la $\mathbb{Z}$ la K). Morfismul φ este cu necesitate injectiv; arătați că este şi morfism de ordine.

7. Demonstrați că relația de ordine uzuală este singura relație de ordine pe $\mathbb{Q}$ în raport cu care acesta devine corp ordonat.

8. Fie K un corp ordonat. Demonstrați că funcția valoare absolută $|\ | : K \to K$ are proprietățile uzuale ale modulului: a) $\forall x \in K \Rightarrow |x| \ge 0$; b) $\forall x \in K$, are loc: $|x| = 0 \Leftrightarrow x = 0$; c) $\forall x, y \in K \Rightarrow |x + y| \le |x| + |y|$ (inegalitatea triunghiulară); d) $\forall x, y \in K \Rightarrow |x\cdot y| = |x|\cdot|y|$.

9. Arătați că nu orice submulțime nevidă majorată a lui $\mathbb{Q}$ are margine superioară.

II.4. Inele de clase de resturi $\mathbb{Z}_n$, inele factor

În mod tradițional, structurile „numerice” $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sînt considerate de bază în matematică; cînd se face referire la noțiunea de „număr”, este de obicei vorba de un element al uneia din aceste mulțimi. Acest loc privilegiat este asigurat, în mare măsură, de rolul important pe care îl au aceste structuri în modelarea lumii reale (deşi numerele complexe au fost mult timp privite ca nişte creații pur abstracte [29]), lucru reflectat în importanța ce li se acordă în manualele de liceu şi gimnaziu.

Considerăm că şi structurile $\mathbb{Z}_n$ (inelele de clase de resturi modulo n) merită să ocupe un loc alături de aceste structuri, măcar din următoarele motive:

- construcția lor riguroasă este intuitivă şi simplă (în comparație cu cea a lui $\mathbb{R}$, de exemplu), iar cunoaşterea lor de către elevi prezintă evidente avantaje didactice.
- generalizarea directă la inele factor deschide calea către metodele algebrei moderne.
- au aplicații semnificative în matematică (mai ales în probleme de divizibilitate).
- calculatoarele, tehnologia informației şi a comunicațiilor digitale (reprezentarea numerelor în calculator, implementarea operațiilor cu ele, codurile corectoare de erori, criptografia, securitatea datelor, …), omniprezente în viața de astăzi, folosesc în mod intens inelele şi corpurile *finite*, între care inelele de tip $\mathbb{Z}_n$ sînt cele mai la îndemînă.

Prezentăm mai întîi, pe scurt, etapele *construcției inelului de clase de resturi modulo n*, $\mathbb{Z}_n$. Apoi vom da construcția generală a inelului factor al unui inel R în raport cu un ideal I al său. Inelele factor intervin în multe alte construcții importante în matematică: corpurile $\mathbb{R}$ şi $\mathbb{C}$, corpurile finite; o construcție asemănătoare celei a lui $\mathbb{R}$ (construit pornind de la $\mathbb{Q}$ şi valoarea absolută uzuală pe $\mathbb{Q}$) permite obținerea corpurilor de numere *p-adice* (pornind de la $\mathbb{Q}$, un număr prim p şi valoarea absolută p-adică pe $\mathbb{Q}$).

Fie n un număr întreg, fixat (numit *modul*).

4.1 Definiție. Spunem că numerele întregi a şi b sînt *congruente modulo n* dacă n divide $a - b$. Scriem aceasta sub forma $a \equiv b \pmod{n}$.

4.2 Propoziție. *Relația „ $\equiv \pmod{n}$” de congruență modulo n este o relație de echivalență pe* $\mathbb{Z}$. □

[29] Vezi, de exemplu, sintagma "număr pur imaginar"…

Pentru orice $a \in \mathbb{Z}$, se notează cu $\hat{a}$ clasa lui a în raport cu relația de congruență modulo n. Avem deci $\hat{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}$. Observăm că notația este ambiguă, în sensul că nu precizează modulul (numărul n); este deci necesară atenție şi notații adecvate pentru evitarea confuziilor ce pot apărea în cazul folosirii mai multor relații de congruență. Mulțimea factor $\mathbb{Z}/\equiv \pmod{n}$ (adică $\{\hat{a} \mid a \in \mathbb{Z}\}$) se notează cu $\mathbb{Z}_n$ şi se numeşte *mulțimea claselor de resturi modulo n*.

4.3 Exercițiu. a) Ce devine relația de congruență modulo n şi mulțimea $\mathbb{Z}_n$ dacă $n = 0$ sau $n = 1$?

b) Două numere întregi a şi b sînt congruente modulo n dacă şi numai dacă „dau acelaşi rest la împărțirea cu n”.

Pe $\mathbb{Z}_n$ se pot defini două operații (numite *adunarea*, respectiv *înmulțirea modulo n*), în raport cu care $\mathbb{Z}_n$ devine *inel comutativ şi unitar*. Pentru orice $a, b \in \mathbb{Z}$, definim:

$$\hat{a} + \hat{b} := \widehat{a + b}$$
$$\hat{a} \cdot \hat{b} := \widehat{a \cdot b}$$

Demonstrarea corectitudinii definițiilor de mai sus (adică independența de alegerea reprezentanților) şi a axiomelor inelului este propusă cititorului.

Vom aplica ideea construcției de mai sus într-o situație mai generală. În acest scop, observăm că putem defini relația de congruență modulo n pe $\mathbb{Z}$ şi în felul următor:

Notăm $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$. Avem atunci, $\forall a, b \in \mathbb{Z}$:

$$a \equiv b \pmod{n} \Leftrightarrow a - b \in n\mathbb{Z}.$$

Mai mult, se vede imediat că $\hat{a} = \{a + nk \mid k \in \mathbb{Z}\}$, motiv pentru care $\hat{a}$ se mai notează cu $a + n\mathbb{Z}$. Deci, $\hat{0} = n\mathbb{Z}$, $\hat{1} = 1 + n\mathbb{Z}$ etc.

Mulțimea $n\mathbb{Z}$ este *ideal în* $\mathbb{Z}$, în sensul că este parte stabilă la adunare şi, $\forall x \in \mathbb{Z}$, $\forall a \in n\mathbb{Z}$, rezultă că $xa \in n\mathbb{Z}$ ($n\mathbb{Z}$ este parte stabilă la înmulțirea cu *orice* element din $\mathbb{Z}$).

Mai general, dacă R este *inel* (presupus pentru simplitate *comutativ şi unitar*), o submulțime nevidă I a sa se numeşte *ideal* în R (fapt notat $I \leq R$) dacă satisface condițiile:

- $\forall a, b \in I$, rezultă $a + b \in I$;
- $\forall a \in I$, $\forall r \in R$, rezultă $ra \in I$.

Se observă imediat că orice ideal I al lui R este subgrup al grupului aditiv $(R, +)$ (demonstrați!) şi deci $0 \in I$. Idealul I se numeşte *propriu* dacă $I \neq R$.

Propoziția următoare arată că ideea de construcție a lui $\mathbb{Z}_n$ pornind de la $\mathbb{Z}$ şi un ideal al său (de forma $n\mathbb{Z}$) se generalizează cuvînt cu cuvînt la cazul unui inel R şi al unui ideal I al său.[30]

[30] Afirmațiile rămîn valabile pentru un inel nu neapărat comutativ R şi un ideal *bilateral* I al lui R.

Demonstrația constă în verificarea directă a proprietăților enunțate şi o lăsăm cititorului (şi poate fi găsită în orice carte introductivă de algebră „modernă”).

4.4 Propoziție. *Fie R un inel comutativ unitar şi I un ideal al său.*

a) Relația (*de* congruență modulo I), *definită de:*

$$a \equiv b \ (\mathrm{mod}\ I) \Leftrightarrow a - b \in I$$

este o relație de echivalență pe I. Notînd cu $\hat{a} = \{b \in R \mid a \equiv b \ (\mathrm{mod}\ I)\}$ (*numită* clasa lui a modulo I), *are loc* $\hat{a} = \{a + x \mid x \in I\}$ ($\hat{a}$ *se mai notează* $a + I$ *din acest motiv*).

b) Relația de congruență modulo I este compatibilă cu adunarea şi înmulțirea din R, *în sensul că*, $\forall a, a', b, b' \in R$, *au loc implicațiile:*

$$a \equiv a' \ (\mathrm{mod}\ I) \text{ şi } b \equiv b' \ (\mathrm{mod}\ I) \Rightarrow a + b \equiv a' + b' \ (\mathrm{mod}\ I) \text{ şi } a \cdot b \equiv a' \cdot b' \ (\mathrm{mod}\ I).$$

c) Operațiile pe mulțimea factor $R/I := \{\hat{a} \mid a \in R\}$, *date de:*

$$\hat{a} + \hat{b} := \widehat{a + b} \text{ şi } \hat{a} \cdot \hat{b} \equiv \widehat{a \cdot b}, \ \forall a, b \in R,$$

sînt corect definite şi înzestrează pe R/I *cu o structură de inel comutativ unitar* (*numit* inelul factor al lui R în raport cu I).

d) Aplicația $\pi : R \to R/I$, $\pi(r) = \hat{r} = r + I$, $\forall r \in R$, *este un morfism surjectiv de inele* (*numit* surjecția canonică a inelului factor R/I). □

În termeni mai puțin riguroşi, trecerea de la inelul R la inelul factor R/I „duce toate elementele din I în zero” sau „anulează elementele lui I”. Multe afirmații referitoare la idealul I în R se traduc prin afirmații referitoare la idealul 0 în R/I (un exemplu este 4.8), idee aplicată adesea în raționamente.

4.5 Observație. Are loc o afirmație reciprocă celei de la *b)*: dacă ρ este o relație de echivalență pe inelul R care este *compatibilă* cu operațiile de pe R ($\forall a, a', b, b' \in R$ cu $a\rho a'$ şi $b\rho b' \Rightarrow (a + b)\rho(a' + b')$ şi $(a \cdot b)\rho(a' \cdot b')$), atunci clasa de echivalență a lui 0 în raport cu ρ (adică $I_\rho := \{a \in R \mid a\rho 0\}$) este ideal în R şi ρ coincide cu relația de congruență modulo I_ρ. Pe de altă parte, o relație de echivalență pe R, cu proprietatea că mulțimea factor poate fi înzestrată cu două operații după regula de la *c)* din propoziția de mai sus, trebuie să fie o relație compatibilă cu structura de inel (pentru a asigura corectitudinea definițiilor!). Apare în acest fel legătura strînsă dintre noțiunea de *ideal* într-un inel şi cea de inel factor.

Este de aşteptat ca un rol esențial în ce priveşte proprietățile inelului factor R/I să îl aibă idealul I. În acest sens, sînt importante următoarele noțiuni:

4.6 Definiție. Fie R un inel comutativ. Un ideal P al lui R se numeşte *ideal prim* dacă $P \neq R$ şi oricare ar fi $x, y \in P$, din $xy \in P$ rezultă $x \in P$ sau $y \in P$. Un ideal M al lui R se numeşte *ideal maximal* dacă $M \neq R$ şi nu există ideale proprii ale lui R care includ strict pe M: pentru orice $J \leq R$, din $M \leq J$ rezultă $M = J$ sau $J = R$.

4.7 Exemple. *a)* Dacă p este un număr întreg prim ($\forall a,\ b \in \mathbb{Z}$, dacă p divide produsul ab, atunci $p|a$ sau $p|b$), atunci idealul generat de p în $\mathbb{Z}$, notat $p\mathbb{Z}$, este ideal prim în $\mathbb{Z}$. Reciproc, dacă $p\mathbb{Z}$ este ideal prim, atunci p este număr prim.

b) Un ideal I este maximal în inelul R dacă este element maximal al mulțimii ordonate (cu incluziunea) a idealelor proprii ale lui R. În inelul $\mathbb{Z}$, orice ideal este de forma $n\mathbb{Z}$, cu $n \in \mathbb{Z}$. De aici rezultă că idealul $n\mathbb{Z}$ este maximal dacă şi numai dacă n este număr prim. Într-adevăr, fie $n\mathbb{Z}$ ideal maximal. Atunci, $\forall m \in \mathbb{Z}$, din $n\mathbb{Z} \subseteq m\mathbb{Z}$ rezultă $n\mathbb{Z} = m\mathbb{Z}$ sau $m\mathbb{Z} = \mathbb{Z}$; cu alte cuvinte, din $m|n$ rezultă $m = \pm n$ sau $m = \pm 1$. Aceasta înseamnă că n este ireductibil (nu are alți divizori decît cei triviali, $\pm n$ şi ± 1), deci prim. Reciproca se obține în acelaşi mod.

c) Inelul R este integru dacă şi numai dacă (0) este ideal prim.

d) Dacă K este corp, (0) este singurul său ideal propriu, deci (0) este şi ideal maximal şi ideal prim.

4.8 Teoremă. *Fie R un inel comutativ şi I un ideal propriu în R.*

a) I este ideal prim dacă şi numai dacă inelul factor R/I este integru (adică 0 *este ideal prim în R/I).*

b) I este ideal maximal dacă şi numai dacă inelul factor R/I este corp (adică 0 *este ideal maximal în R/I).*

Demonstrație. *a)* Fie I un ideal prim. Fie $\alpha = a + I$, $\beta = b + I$ (cu $a,\ b \in R$) elemente din R/I. Dacă $\alpha\beta = 0$, atunci $(a + I)(b + I) = 0 + I$, adică $ab \in I$. Cum I este prim, obținem $a \in I$ sau $b \in I$, adică $a + I = \alpha = 0 + I$ sau $b + I = \beta = 0 + I$. Aşadar, R/I este integru. Reciproc, presupunem că R/I este integru şi fie a, $b \in R$ cu $ab \in I$. Aceasta înseamnă că $(a + I)(b + I) = 0 + I$, deci $a + I = 0 + I$ sau $b + I = 0 + I$. Astfel, $a \in I$ sau $b \in I$.

b) Presupunem că I este ideal maximal în R. Vrem să arătăm că orice element nenul al inelului R/I este inversabil. Fie deci $\alpha = a + I$, cu $\alpha \neq 0 + I$, deci $a \notin I$. Atunci idealul generat de I şi a, adică $I + Ra$, include strict pe I; din maximalitatea lui I obținem $I + Ra = R$. În particular, $1 \in R$ se scrie sub forma $i + ra$, cu $i \in I$ şi $r \in R$. Avem deci $1 + I = (ra + i) + I = ra + I = (r + I)(a + I)$, ceea ce arată că $a + I$ este inversabil. Fie acum R/I corp şi J un ideal care include strict pe I. Există aşadar $x \in J$, $x \notin I$. Aceasta înseamnă că $x + I \neq 0 + I$, deci $x + I$ este inversabil în R/I. Putem scrie atunci $1 + I = (r + I)(x + I)$, cu $r \in R$, adică există $i \in I$ astfel încît $1 = rx + i$. De aici rezultă că $1 \in J$, adică $J = R$. □

Propoziția de mai sus dă un procedeu simplu şi valoros, des utilizat, de a *construi corpuri ca inele factor în raport cu ideale maximale*. Această metodă apare, între altele, la construcțiile corpurilor finite, a lui $\mathbb{R}$ şi $\mathbb{C}$. De exemplu, $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, inelul claselor de resturi modulo p (unde p este un număr prim) este un corp finit.

4.9 Observație. a) Idealul I este maximal în R dacă şi numai dacă $\forall x \in R$ cu $x \notin I$, rezultă că $\exists i \in I$ şi $r \in R$ astfel încît $i + rx = 1$ (vezi demonstrația precedentă).

b) Dacă $\varphi : R \to S$ este un morfism surjectiv de inele, atunci există o corespondență bijectivă, care păstrează incluziunile, între idealele lui R care includ Kerφ şi idealele lui S. Corespondența asociază idealului J în R idealul $\varphi(J)$ (imaginea lui J prin φ), care este ideal în S. Aplicînd această afirmație situației în care I este ideal maximal în R şi surjecției canonice $\pi : R \to R/I$ (cu Ker$\pi = I$), rezultă că R/I nu are ideale proprii în afară de 0 şi R/I (căci singurele ideale în R care să includă pe I sînt I şi R). Dar un inel comutativ care nu are alte ideale în afară de 0 şi inelul însuşi este corp (demonstrați!).

4.10 Corolar. *Orice ideal maximal este prim.* □

Reciproca este falsă: idealul (X) al inelului $\mathbb{Z}[X]$ este prim şi nu este maximal, după cum se vede considerînd inelul factor: $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$, care e integru dar nu e corp. Propunem cititorului să demonstreze aceste fapte cu ajutorul definițiilor.

Tot în legătură cu idealele maximale, are loc următorul rezultat, care foloseşte în mod esențial Lema lui Zorn:

4.11 Teoremă. (Lema lui Krull[31]) *Fie R un inel unitar comutativ. Atunci orice ideal propriu al lui R este inclus într-un ideal maximal. În particular, R are ideale maximale.*

Demonstrație. Fie $I \le_R R$, $I \ne R$. Notăm cu **P** mulțimea idealelor *proprii* ale lui R, care includ pe I. **P** este o mulțime ordonată cu incluziunea; elementele ei maximale (dacă există!) sînt exact idealele maximale ale lui R, care includ pe I. Vom folosi lema lui Zorn pentru a demonstra existența elementelor maximale în **P**. Fie deci un lanț $(E_j)_{j\in J}$, cu $E_j \in$ **P**, $\forall i \in J$. Acest lanț de ideale are un majorant în **P**, anume $\bigcup_{j\in J} E_j =: E$. Într-adevăr, E este ideal[32]: dacă $x, y \in E$, atunci există $i, j \in J$ cu $x \in E_i$, $y \in E_j$; cum $(E_j)_{j\in J}$ este lanț, rezultă că $E_i \subseteq E_j$ sau $E_j \subseteq E_i$. Deci $x - y \in E_j$ (căci $E_j \le_R R$) sau $x - y \in E_i$. În orice caz, $x - y \in E$. La fel se demonstrează că $\forall r \in R$, $\forall x \in E$, rezultă $rx \in E$. Deci E este ideal, care include evident pe I.

Trebuie să demonstrăm şi că $E \ne R$. Dacă, prin absurd, $E = R$, atunci $1 \in E = \bigcup_{j\in J} E_j$, deci există $j \in J$ cu $1 \in E_j$. Însă atunci $E_j = R$, contradicție cu $E_j \in$ **P** (E_j este ideal propriu!).

Din lema lui Zorn, există un element maximal al lui **P**.

Luînd $I = 0$, rezultă existența unui ideal maximal în R. □

Aplicații la criterii de divizibilitate. Utilizarea congruențelor (a inelelor de resturi) modulo n) conduce la demonstrarea rapidă (şi chiar fabricarea) de criterii de divizibilitate pentru numere scrise într-o anumită bază (de obicei baza 10). Iată un exemplu binecunoscut:

---

[31] Wolfgang Adolf Ludwig Helmuth Krull (1899-1971), matematician german cu importante contribuții în algebră.

[32] În general, reuniunea unei familii oarecare de ideale *nu* este ideal.

4.12 Propoziție. (*Criteriul de divizibilitate cu* 3) *Un număr scris în baza* 10 *este divizibil cu* 3 *dacă şi numai dacă suma cifrelor sale este divizibilă cu* 3.

Demonstrație. Fie $a = \overline{c_{n-1}\ldots c_1c_0}$ un număr în baza 10, cu $c_i \in \{0, \ldots, 9\}$. Vom demonstra, mai general, că $a \equiv \sum c_i$ (mod 3). Dar (toate congruențele sînt modulo3):

$$a \equiv \sum c_i 10^i \equiv \sum c_i 1^i \equiv \sum c_i,$$

căci $10 \equiv 1$ (mod 3). □

Ideea care stă la baza tuturor criteriilor de divizibilitate cu d pentru numere scrise în baza b este aceeaşi cu cea de mai sus: fiind dat $a = \overline{c_{n-1}\ldots c_1c_0}$ în baza b, se calculează $a \equiv \sum_{i \geq 0} c_i b^i$ (mod d). Pentru aceasta, se calculează b^i modulo d, pentru $i = 0, 1, \ldots$. Se poate demonstra că acest şir este periodic (cu posibila excepție a unui număr finit de termeni), adică există $k, t \in \mathbb{N}$, $t > 0$, astfel încît $b^i \equiv b^{i+t}$(mod d), $\forall i \geq k$.

4.13 Exerciții. a) (Criteriul de divizibilitate cu 9) Un număr scris în baza 10 este divizibil cu 9 dacă şi numai dacă suma cifrelor sale este divizibilă cu 9.

b) (Criteriul de divizibilitate cu 2, respectiv 5, respectiv 10) Un număr scris în baza 10 este divizibil cu 2 (respectiv 5, respectiv 10) dacă şi numai dacă ultima sa cifră (c_0) este divizibilă cu 2 (respectiv 5, respectiv 10).

c) Generalizați a) şi b) pentru o bază oarecare b.

d) (Criteriul de divizibilitate cu 7)[33] Restul împărțirii la 7 a unui număr $\overline{c_{n-1}\ldots c_1c_0}$ scris în baza 10 este acelaşi cu restul împărțirii la 7 a lui $c_0 + 3c_1 + 2c_2 - c_3 + 4c_4 + 5c_5 + c_6 + 3c_7 + \ldots$

4.14 Teoremă. (Lema chineză a resturilor) *Fie R inel comutativ,* $n \geq 2$ *şi* $I_1, \ldots, I_n$ *ideale ale lui R.*

a) Dacă $I_i + I_j = R$ *pentru* $i \neq j$,[34] *atunci produsul*[35] $I_1 \cdot \ldots \cdot I_n$ *este egal cu intersecția* $I_1 \cap \ldots \cap I_n$ *şi există un izomorfism natural de inele (şi de R-module):*

$$\frac{R}{I_1 \cdot \ldots \cdot I_n} = \frac{R}{I_1 \cap \ldots \cap I_n} \cong \frac{R}{I_1} \times \ldots \times \frac{R}{I_n}, \; r + I_1 \cap \ldots \cap I_n \mapsto (r + I_1, \ldots, r + I_n), \forall r \in R.$$

b) Reciproc, dacă morfismul $\varphi : R \to \frac{R}{I_1} \times \ldots \times \frac{R}{I_n}$, $\varphi(r) = (r + I_1, \ldots, r + I_n)$, $\forall r \in R$ *este surjectiv (inducînd un izomorfism* $\frac{R}{I_1 \cap \ldots \cap I_n} \cong \frac{R}{I_1} \times \ldots \times \frac{R}{I_n}$*, ca mai sus), atunci idealele* I_i *şi* I_j *sînt comaximale pentru* $i \neq j$.

---

[33] Utilitatea practică acestui criteriu este discutabilă…

[34] Idealele I_i şi I_j se numesc în acest caz *comaximale*. De exemplu, idealele $\mathbb{Z}a$ şi $\mathbb{Z}b$ ale lui $\mathbb{Z}$ sînt comaximale dacă şi numai dacă a şi b sînt prime între ele.

[35] Reamintim că *produsul IJ* a două ideale I şi J este idealul *generat* de mulțimea produselor ij, cu $i \in I, j \in J$. Se arată uşor că produsul de ideale este asociativ şi că întotdeauna $IJ \subseteq I \cap J$.

Demonstrație. *a)* Aplicăm o inducție după n pentru a demonstra că $I_1\cdot\ldots\cdot I_n = I_1\bigcap\ldots\bigcap I_n$ şi că are loc izomorfismul cerut. Pentru $n = 2$, din $I_1 + I_2 = R$ deducem că există $x \in I_1$, $y \in I_2$ astfel încît $x + y = 1$. Fie $z \in I_1\bigcap I_2$. Atunci $z = z\cdot 1 = zx + zy$, cu zx, $zy \in I_1\cdot I_2$, adică $I_1\bigcap I_2 \subseteq I_1I_2$. Astfel, $I_1\bigcap I_2 = I_1I_2$.

Fie $\varphi : R \to \dfrac{R}{I_1}\times\dfrac{R}{I_2}$, $\varphi(r) = (r + I_1,\ r + I_2)$, $\forall r \in R$. E uşor de văzut că φ este morfism de inele şi de R-module (este produsul direct al surjecțiilor canonice $R \to R/I_j$). Avem $\mathrm{Ker}\varphi = \{r \in R|\ (r + I_1,\ r + I_2) = (0 + I_1,\ 0 + I_2)\} = I_1\bigcap I_2$; teorema de izomorfism asigură că $R/I_1\bigcap I_2 \cong \mathrm{Im}\varphi$. E suficient aşadar să demonstrăm surjectivitatea lui φ. Fie $(r_1 + I_1,\ r_2 + I_2) \in \dfrac{R}{I_1}\times\dfrac{R}{I_2}$. Trebuie să găsim $r \in R$ cu $r - r_1 \in I_1$, $r - r_2 \in I_2$. Un astfel de element este $r = r_1 y + r_2 x$. Într-adevăr,

$$r - r_1 = r_1y + r_2x - r_1x - r_1y = (r_2 - r_1)x \in I_1.$$

Analog se arată că $r - r_2 \in I_2$.

Presupunem că pentru orice $k < n$ şi orice ideale $I_1,\ldots, I_k$, comaximale două cîte două, are loc $I_1\cdot\ldots\cdot I_k = I_1\bigcap\ldots\bigcap I_k$ şi are loc izomorfismul cerut. Fie n ideale $I_1,\ldots, I_n$ ca în enunț. Din $I_j + I_n = R$, $1 \le j \le n - 1$, rezultă că există $a_j \in I_j$, $b_j \in I_n$ astfel încît $a_j + b_j = 1$. Înmulțind aceste $n - 1$ egalități membru cu membru obținem

$$\prod_{j=1}^{n-1}\left(a_j + b_j\right) = a_1\cdot\ldots\cdot a_{n-1} + b = 1, \text{ unde } b \in I_n,\ a_1\cdot\ldots\cdot a_{n-1} \in I_1\cdot\ldots\cdot I_{n-1}.$$

Deci $I_1\cdot\ldots\cdot I_{n-1} + I_n = R$. Aplicînd cazul $n = 2$ idealelor comaximale $I_1\cdot\ldots\cdot I_{n-1}$ şi I_n, rezultă că $I_1\cdot\ldots\cdot I_{n-1}\cdot I_n = (I_1\cdot\ldots\cdot I_{n-1})\bigcap I_n = (I_1\bigcap\ldots\bigcap I_{n-1})\bigcap I_n$ (am folosit şi ipoteza de inducție $I_1\cdot\ldots\cdot I_{n-1} = I_1\bigcap\ldots\bigcap I_{n-1}$). Mai rezultă că:

$$\frac{R}{\left(I_1\cdot\ldots\cdot I_{n-1}\right)\cdot I_n} \cong \frac{R}{I_1\cdot\ldots\cdot I_{n-1}}\times\frac{R}{I_n} \text{ prin } r + I_1\cdot\ldots\cdot I_n \mapsto (r + I_1\ldots I_{n-1},\ r + I_n),\ \forall r \in R.$$

Folosind ipoteza de inducție, avem izomorfismul:

$$\frac{R}{I_1\cdot\ldots\cdot I_{n-1}} \cong \frac{R}{I_1}\times\ldots\times\frac{R}{I_{n-1}} \text{ prin } r + I_1\cdot\ldots\cdot I_{n-1} \mapsto (r + I_1,\ \ldots r + I_{n-1}),\ \forall r \in R.$$

Combinînd aceste izomorfisme, obținem rezultatul din enunț.

b) Vom demonstra că I_1 şi I_2 sînt comaximale. Fie $(1 + I_1,\ 0 + I_2,\ \ldots,\ 0 + I_n) \in \dfrac{R}{I_1}\times\ldots\times\dfrac{R}{I_n}$. Există $y \in R$ astfel încît $(y + I_1,\ y + I_2,\ \ldots,\ y + I_n) = (1 + I_1,\ 0 + I_2,\ \ldots,\ 0 + I_n)$, adică $y \in I_2$ şi $y - 1 =: x \in I_1$. Deci $1 = -x + y \in I_1 + I_2$, adică $I_1 + I_2 = R$. □

4.15 Exemplu. În $\mathbb{Z}$, idealele $a\mathbb{Z}$ şi $b\mathbb{Z}$ sînt comaximale $\Leftrightarrow$ $(a,\ b) = 1$. Avem în acest caz, conform lemei chineze a resturilor, $\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ (cu notațiile clasice pentru inelele de clase de resturi $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$, izomorfismul fiind dat de $x + ab\mathbb{Z} \mapsto (x + a\mathbb{Z},\ x + b\mathbb{Z})$. În particular, pentru orice pereche de numere naturale $(c,\ d)$ cu $0 \le c < a$, $0 \le d < b$, există un unic x, $0 \le x < ab$, astfel încît $x \equiv c \pmod a$ şi $x \equiv d \pmod b$.

II.5. Corpul numerelor reale

Necesitatea introducerii numerelor întregi şi a celor raţionale este aproape evidentă din experienţa imediată. Nu acesta este cazul numerelor reale, care au apărut din raţiuni mai profunde. Descoperirea de către matematicienii Greciei antice că diagonala pătratului de lungime 1 nu poate fi exprimată ca un raport de numere întregi (în termeni moderni, $\sqrt{2} \notin \mathbb{Q}$) a condus la o adevărată criză a ştiinţei şi filozofiei în acea vreme.

Imaginea intuitivă cea mai simplă despre $\mathbb{R}$, care reflectă cel mai bine structura de ordine, este cea a punctelor de pe o *dreaptă* (alt concept abstract, dar mai accesibil gîndirii), unde s-a fixat un punct O (*originea*, corespunzînd lui 0) şi un alt punct U, diferit de primul (corespunzător lui 1 şi avînd rolul de a fixa unitatea de măsură pe acea dreaptă). Orice număr real corespunde în mod unic unui punct de pe dreaptă: numărul real corespunzător punctului P este *distanţa* de la O la P (dacă P este de aceeaşi parte ca şi U faţă de O), respectiv distanţa de la O la P luată cu semnul minus dacă O este între U şi P. Se conturează astfel ideea intuitivă că numerele reale „pot măsura orice distanţă”. Este semnificativ acest punct de vedere dacă se observă rolul esenţial pe care îl are $\mathbb{R}$ în definiţia generală a *spaţiilor metrice* (spaţii în care este definită o noţiune de *distanţă*).

În multe cărţi (între care şi manualele de Analiză de liceu) structura numerelor reale este dată „axiomatic”: se numeşte *corp al numerelor reale* un *corp comutativ* $(\mathbb{R}, +, \cdot)$ înzestrat cu o relaţie de *ordine totală* " $\leq$ ", satisfăcînd proprietăţile:

R1. $\mathbb{R}$ este *corp ordonat*, adică $\forall a, b, c \in \mathbb{R}$ au loc:

$$a \leq b \Rightarrow a + c \leq b + c;$$

$$a \leq b \text{ şi } c \geq 0 \Rightarrow ac \leq bc.$$

R2. Orice submulţime nevidă majorată a lui $\mathbb{R}$ are margine superioară.

Evident, această definiţie ridică două probleme: *existenţa* unei structuri cu proprietăţile de mai sus şi *unicitatea* sa. Unicitatea este tranşată de următorul rezultat:

5.1 Teoremă. *Pentru orice două corpuri comutative ordonate* $(K, +, \cdot, \leq)$ *şi* $(L, +, \cdot, \leq)$ *care satisfac proprietatea* R2 *există un unic izomorfism de corpuri* $\varphi : K \to L$, *care este şi izomorfism de ordine:* $\forall x, y \in K, x \leq y \Rightarrow \varphi(x) \leq \varphi(y)$. □

Problema existenţei se rezolvă printr-o *construcţie efectivă* a lui $\mathbb{R}$, presupunînd dat $\mathbb{Q}$. Cele mai cunoscute procedee sînt *construcţia zecimală*, *construcţia prin tăieturi în* $\mathbb{Q}$ şi *construcţia cu ajutorul şirurilor Cauchy* (şiruri *fundamentale*). Construcţia folosind şirurile Cauchy prezintă avantajele eleganţei şi rapidităţii şi se foloseşte şi la alte construcţii importante: *completatul unui corp normat oarecare, completatul unui spaţiu metric, completatul unui spaţiu vectorial normat*.

Pentru edificarea cititorului, vom schiţa construcţia zecimală şi apoi prezentăm construcţia cu şirurile Cauchy. Construcţia prin tăieturi, aparţinînd lui Dedekind, este descrisă la exerciţii.

Construcția zecimală a lui $\mathbb{R}$ (datorată lui Weierstrass[36]) identifică un număr real cu o „fracție zecimală infinită”. De exemplu,

1,4142135623730950488016887242097…, 3,1415926535897932384626433832795…

sînt numerele reale $\sqrt{2}$, respectiv π (de fapt, e vorba de „trunchieri” ale lor; nu am scris *toate* zecimalele, din motive evidente de spațiu…;). Formal, se consideră mulțimea :

$$\mathfrak{R} = \{b_0,b_1b_2\ldots b_n\ldots \mid b_0 \in \mathbb{Z}, b_i \in \{0, 1, \ldots, 9\}, \forall i \in \mathbb{N}^*\}$$

Interpretarea intuitivă este: „$b_0,b_1b_2\ldots b_n\ldots$ este suma seriei $b_0 + \sum_{n\geq 1} b_i \cdot 10^{-i}$” (dar, evident, nu putem *defini* astfel un număr real. De ce?).

Alegerea lui 10 ca bază este mai degrabă legată de tradiție, în locul său putînd fi ales orice număr natural $b \geq 2$ (evident, avem atunci $b_i \in \{0, 1, \ldots, b-1\}$, adică b_i sînt cifre în baza b).

Apar însă probleme : 0,9999… , scris şi ca 0,(9) („cu perioada 9”) este de fapt 1 (formal 1,000…), după cum se vede făcînd suma seriei corespunzătoare; cum nu dorim ca un acelaşi număr real să aibă două reprezentări zecimale distincte, trebuie făcută următoarea „identificare”: orice şir de forma $b = b_0,b_1b_2\ldots b_n\ldots$, cu proprietatea că $\exists k \geq 0$ astfel încît $b_i = 9$, $\forall i > k$ şi $b_k < 9$, este identificat cu şirul $b_0,b_1b_2\ldots(b_k + 1)000\ldots$ (dacă $k \geq 1$), respectiv cu $(b_0 + 1),000\ldots$ (dacă $k = 0$). Pentru rigurozitate, se defineşte o relație de echivalență ~ pe $\mathfrak{R}$, ca mai sus, iar mulțimea factor $\mathfrak{R}/\sim$ va fi prin definiție $\mathbb{R}$. Alte dificultăți apar la definirea adunării şi înmulțirii a două fracții zecimale infinite (de fapt a unor clase de echivalență din $\mathfrak{R}/\sim$), fiind necesară apelarea la operațiile pe „trunchierile raționale” ale şirurilor respective şi la definirea unei noțiuni de limită în $\mathfrak{R}/\sim$. Invităm cititorul să încerce să dea singur aceste definiții şi să demonstreze pe baza lor proprietățile uzuale ale operațiilor cu numere reale, pentru a măsura dificultățile construcției. Avantajele acestei abordări (în măsura detalierii efective de către cititor!) constau în apropierea de imaginea intuitivă a conceptului de număr real şi la definirea *relației de ordine*, care coincide cu cea *lexicografică*[37]: se defineşte $b_0,b_1b_2\ldots b_n\ldots < c_0,c_1c_2\ldots c_n\ldots \Leftrightarrow \exists k \in \mathbb{N}$ astfel încît $b_k < c_k$ şi, $\forall i < k$, are loc $b_i = c_i$.

Construcția lui $\mathbb{R}$ cu ajutorul şirurilor Cauchy (G. Cantor)

$\mathbb{Q}$ este un *corp normat*. Mai precis, aplicația *valoare absolută* (sau *modùl*) $|\cdot| : \mathbb{Q} \to \mathbb{Q}$,

$$|x| = \begin{cases} x & \text{dacă } x \geq 0 \\ -x & \text{dacă } x < 0 \end{cases}$$

are proprietățile (binecunoscute) următoare:

N1. $\forall x \in \mathbb{Q}$ are loc $|x| \geq 0$.

N2. $\forall x \in \mathbb{Q}$ are loc $|x| = 0 \Leftrightarrow x = 0$.

N3. $\forall x, y \in \mathbb{Q}$ are loc $|x + y| \leq |x| + |y|$ (inegalitatea triunghiulară).

N4. $\forall x, y \in \mathbb{Q}$ are loc $|x \cdot y| = |x| \cdot |y|$.

---

36 Karl Theodor Wilhelm Weierstrass (1815-1897), matematician german, considerat "părintele analizei moderne".

37 Lexicon = dicționar. Puteți spune de ce se numeşte aşa ordinea definită?

Altfel spus, valoarea absolută este o *normă*[38]. Cu ajutorul normei definim o *distanță* (o *metrică*)[39], adică o aplicație $d : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, $d(x, y) := |x - y|$, $\forall (x, y) \in \mathbb{Q}$, cu proprietățile:

D1. $\forall x, y \in \mathbb{Q}$ are loc $d(x, y) = d(y, x) \geq 0$.

D2. $\forall x, y \in \mathbb{Q}$ are loc $d(x, y) = 0 \Leftrightarrow x = 0$.

D3. $\forall x, y, z \in \mathbb{Q}$ are loc $d(x, y) \leq d(x, z) + d(z, y)$ (inegalitatea triunghiulară).

Ca o consecință, se obține $|x - y| \geq ||x| - |y||$, $\forall x, y \in \mathbb{Q}$.

Metrica determină o *topologie*[40] pe $\mathbb{Q}$. Proprietățile metrice şi topologice ale lui $\mathbb{Q}$ nu sînt prea bune, tocmai din cauzele amintite la început: nu orice şir de numere raționale „care ar trebui să fie convergent la ceva” este convergent la un număr rațional (de exemplu, şirul aproximărilor zecimale ale lui $\sqrt{2}$).

Construcția lui $\mathbb{R}$ cu şiruri Cauchy porneşte de la ideea că un număr real este o „limită a unui şir de numere raționale”. În loc să ne îndreptăm atenția asupra unui tip particular de şiruri de numere raționale, ca la construcția zecimală (şirurile cu termen general de forma $b_0 + \sum_{i=1}^{n} b_i \cdot 10^{-i}$), se consideră *toate* şirurile de numere raționale $(x_n)_{n \geq 1}$ „care au o limită, nu neapărat în $\mathbb{Q}$”.

Bineînțeles, nu orice şir de numere raționale „are o limită” în sens intuitiv (de exemplu şirul $((-1)^n)_{n \geq 1}$). Pe de altă parte, nu putem defini „existența limitei” şirului (x_n) direct ($\exists l$ astfel încît $x_n \to l$), căci l este în general un număr real, concept pe care tocmai îl construim! Din fericire, ştim de la Analiză că *şirurile care au limită în* $\mathbb{R}$ *sînt exact şirurile Cauchy* (noțiune în care *nu apare explicit* limita şirului).

5.1 Definiție. Şirul de numere raționale $(x_n)_{n \geq 1}$ se numeşte *şir Cauchy* (sau *şir fundamental*) dacă satisface condiția:

$$\forall \varepsilon \in \mathbb{Q}, \varepsilon > 0 \Rightarrow \exists N \in \mathbb{N} \text{ astfel încît } \forall m, n \geq N \text{ să aibă loc } |x_m - x_n| < \varepsilon.$$

Fie $\mathcal{C} := \{(x_n)_{n \geq 1} \mid x_n \in \mathbb{Q}, \forall n \geq 1, (x_n)_{n \geq 1} \text{ şir Cauchy}\}$.

Putem aplica acum ideea intuitivă expusă la început şi să definim două şiruri $(x_n), (y_n) \in \mathcal{C}$ ca fiind *echivalente*[41] dacă „au aceeaşi limită”. Şi această idee se poate exprima fără a invoca explicit valoarea limitei:

$$(x_n)_n \sim (y_n)_n \Leftrightarrow \forall \varepsilon \in \mathbb{Q}, \varepsilon > 0 \Rightarrow \exists N \in \mathbb{N} \text{ astfel încît } \forall n \geq N \text{ să aibă loc } |x_n - y_n| < \varepsilon. \quad (R)$$

În sfîrşit, definim un *număr real* ca o *clasă de echivalență de şiruri din* $\mathcal{C}$; mai precis, mulțimea factor $\mathcal{C}/\sim$ o notăm cu $\mathbb{R}$ şi o numim *mulțimea numerelor reale*. Se observă că orice

---

[38] În general, o *normă* ia valori în $\mathbb{R}$, pe care nu l-am construit încă… , deci titulatura este puțin forțată.

[39] Aceeaşi observație ca mai sus: o *distanță* ia în general valori reale.

[40] Nu mai definim topologia, vezi orice manual de Analiză elementară.

[41] Adică "definesc" acelaşi număr real.

număr rațional a poate fi identificat cu clasa în $\mathcal{C}/\sim$ a *şirului constant* $(a, a,\ldots) \in \mathcal{C}$ (adică am obținut într-adevăr o *extindere* a lui $\mathbb{Q}$).

Rămîn sarcinile: de a *defini operațiile*, de a demonstra *corectitudinea definițiilor* şi de a *verifica axiomele de corp comutativ* pentru $\mathbb{R}$. Apoi trebuie definită *relația de ordine* şi arătat că: $\mathbb{R}$ este *total ordonat*, *relația de ordine este compatibilă cu structura de corp şi orice submulțime nevidă majorată are margine superioară*.

Aceste sarcini se pot uşura considerabil dacă folosim instrumente algebrice elementare: *ideale* şi *inele factor*. Observăm că $\mathcal{C}$ este *inel comutativ unitar* şi că $(x_n)_n \sim (y_n)_n \Leftrightarrow (x_n - y_n) \to 0$ (unde scriem $(z_n) \to 0$ dacă $\forall \varepsilon \in \mathbb{Q}$, $\varepsilon > 0 \Rightarrow \exists N \in \mathbb{N}$ astfel încît $\forall n \geq N$ să aibă loc $|z_n| < \varepsilon$). Dacă notăm

$$\mathcal{Z} := \{(z_n)_{n\geq 1} \in \mathcal{C} \mid (z_n) \to 0\},$$

se demonstrează că $\mathcal{Z}$ este *ideal maximal* în $\mathcal{C}$ (şi relația "~" coincide cu relația de congruență modulo $\mathcal{Z}$). Rezultă imediat atunci că $\mathbb{R} = \mathcal{C}/\mathcal{Z}$ este corp comutativ şi cu aceasta se încheie partea „algebrică” a construcției lui $\mathbb{R}$. Notăm cu $[(x_n)]$ imaginea în $\mathcal{C}/\mathcal{Z}$ a şirului $(x_n) \in \mathcal{C}$. Sumarizăm construcția în următoarea:

5.2 Teoremă. *a) Mulțimea $\mathcal{C}$ a şirurilor Cauchy de numere raționale este un inel comutativ unitar*[42] *în raport cu operațiile de adunare şi înmulțire definite „punctual”:*

$$(x_n)_n + (y_n)_n := (x_n + y_n)_n,$$
$$(x_n)_n\cdot(y_n)_n := (x_n\cdot y_n)_n,$$

$\forall (x_n), (y_n) \in \mathcal{C}$.

b) Mulțimea $\mathcal{Z} = \{(z_n)_{n\geq 1} \in \mathcal{C} \mid (z_n) \to 0\}$ a şirurilor din $\mathcal{C}$ care au limita 0 *este un ideal maximal în $\mathcal{C}$, deci inelul factor $\mathcal{C}/\mathcal{Z} =: \mathbb{R}$ este corp comutativ.*

c) Pentru orice $a \in \mathbb{Q}$, considerăm „şirul constant” $(a_n)_n \in \mathcal{C}$, $a_n = a$, $\forall n \in \mathbb{N}^*$. Aplicația care asociază lui $a \in \mathbb{Q}$ clasa în $\mathcal{C}/\mathcal{Z} = \mathbb{R}$ a şirului constant $(a_n)_n$ este un morfism de corpuri. Clasa $[(a_n)] \in \mathbb{R}$ a şirului constant (a_n) va fi numită prin abuz „numărul rațional a”.

d) Definim pe $\mathcal{C}/\mathcal{Z}$ relația binară " < " :

$$[(x_n)] < [(y_n)] \Leftrightarrow \exists \varepsilon \in \mathbb{Q},\ \varepsilon > 0 \text{ şi } \exists N \in \mathbb{N} \text{ astfel încît } x_n + \varepsilon \leq y_n,\ \forall n \geq N.$$

Atunci " < " este bine definită (nu depinde de reprezentanți) şi este o relație de ordine strictă pe $\mathcal{C}/\mathcal{Z}$ (ireflexivă şi tranzitivă). Relația de ordine nestrictă asociată, notată " ≤ ", este o relație de ordine totală pe $\mathbb{R}$; mai mult, $\mathbb{R}$ devine corp ordonat în raport cu această ordine.

e) (Valoarea absolută pe $\mathbb{R}$) Fie $|\cdot| : \mathbb{R} \to \mathbb{R}, |[(x_n)]| = [(|x_n|)]$, $\forall (x_n) \in \mathcal{C}$. Definiția este corectă şi au loc proprietățile normei N1-N4 *de mai sus (bineînțeles, $\mathbb{Q}$ este înlocuit cu $\mathbb{R}$).*

f) Orice şir Cauchy $(r_n)_{n\geq 1}$ de numere reale este convergent la un număr real.[43]

g) Orice submulțime nevidă majorată a lui $\mathbb{R}$ are margine superioară.

---

[42] Este şi integru?
[43] Lăsăm cititorului sarcina de a defini noțiunile de şir Cauchy şi de limită în $\mathbb{R}$.

h) $\mathbb{Q}$ *este dens în* $\mathbb{R}$ (*orice număr real este limita unui şir de numere raţionale*).

Demonstraţie. *a)* Demonstrarea faptului că suma şi produsul a două şiruri Cauchy este tot şir Cauchy este un exerciţiu elementar de Analiză (cf. demonstraţia la „suma, resp. produsul, a două şiruri convergente este un şir convergent"). Este utilă demonstrarea în prealabil a faptului că orice şir Cauchy (x_n) este mărginit ($\exists M \in \mathbb{Q}$ astfel încît $|x_n| \le M$, $\forall n \in \mathbb{N}^*$). Care este elementul nul, respectiv unitate, în $\mathcal{C}$?

b) $\mathcal{Z}$ este ideal: argument standard de Analiză, ca la punctul precedent (se adaptează demonstraţia proprietăţilor $\lim(x_n + y_n) = \lim x_n + \lim y_n$, $\lim(x_n \cdot y_n) = \lim x_n \cdot \lim y_n$).

$\mathcal{Z}$ este maximal: dacă $(x_n) \in \mathcal{C} \setminus \mathcal{Z}$, atunci există $N \in \mathbb{N}$ şi $\delta > 0$ astfel încît $|x_n| > \delta$, $\forall n \ge N$. Într-adevăr, cum (x_n) nu tinde la 0, $\exists \varepsilon > 0$ astfel încît $\forall n \in \mathbb{N}$, $\exists k_n > n$ astfel încît $|x_{k_n}| > \varepsilon$. Însă (x_n) este Cauchy, deci, pentru $\varepsilon/2$, există $N \in \mathbb{N}$ astfel încît $\forall m, n \ge N$, $|x_n - x_m| < \varepsilon/2$. Fie $m = k_N$ dat de proprietatea precedentă. Atunci, $\forall n \ge N$,

$$|x_n| = |x_m + x_n - x_m| \ge |x_m| - |x_n - x_m| > \varepsilon - \varepsilon/2 = \varepsilon/2.$$

Raţionamentul, ca şi multe altele de acelaşi gen, se vede mai bine (şi poate fi intuit!) reprezentînd numerele pe axă.

Revenind la (x_n), rezultă că $\exists N \in \mathbb{N}$ astfel încît $x_n \ne 0$ dacă $n \ge N$. Definim atunci şirul (y_n) prin: $y_n = 0$ dacă $n < N$ şi $y_n = 1/x_n$ dacă $n \ge N$. Şirul (y_n) este Cauchy (demonstraţi!) şi $x_n y_n = 1 + z_n$, unde z_n este 0 pentru $n \ge N$, deci $(z_n) \in \mathcal{Z}$.

e) Trebuie arătat mai întîi că $(|x_n|)$ este şir Cauchy şi că definiţia nu depinde de reprezentanţi. Demonstraţia proprietăţilor normei se face apelînd la proprietăţile corespunzătoare pentru norma în $\mathbb{Q}$.

f) Argumentul este tipic de Analiză, dar îl includem, fiind mai delicat. Fie $(r_n)_{n \ge 1}$ un şir Cauchy de numere reale. Fie $r_n = [(r_{nk})_{k \ge 1}]$, unde $(r_{nk})_{k \ge 1}$ este un şir Cauchy de numere raţionale (pentru orice n fixat). Notăm $r_{nk} =: r(n, k)$, $\forall n, k \ge 1$. Vom arăta că $(r_n)_{n \ge 1}$ are limită în $\mathbb{R}$, anume $[(r(i_n, j_n)_{n \ge 1}]$, unde i_n, j_n sînt nişte şiruri strict crescătoare de numere naturale pe care le definim inductiv, astfel:

Cum $(r_n)_{n \ge 1}$ este şir Cauchy în $\mathbb{R}$, pentru $\varepsilon = 1/4$, $\exists i_1 \in \mathbb{N}$ astfel încît $\forall s, t \ge i_1$ avem $|r_s - r_t| < 1/4$.

Cum $(r_{i_1 k})_{k \ge 1}$ e şir Cauchy în $\mathbb{Q}$, $\exists j_1 \in \mathbb{N}$ astfel încît $|r(i_1, u) - r(i_1, v)| < 1/4$, $\forall u, v \ge j_1$.

Fie $n \in \mathbb{N}$, $n \ge 2$ şi presupunem că am definit $i_1 < i_2 < \ldots < i_{n-1}$ şi $j_1 < j_2 < \ldots < j_{n-1}$, numere naturale astfel încît, $\forall k \in \{1, \ldots, n-1\}$:

$$|r_s - r_t| < 1/2^{k+1}, \forall s, t \ge i_k \text{ (inegalitate în } \mathbb{R}) \quad (1)$$

$$|r(i_k, u) - r(i_k, v)| < 1/2^{k+1}, \forall u, v \ge j_k \quad (2)$$

$$|r(i_k, u) - r(i_{k-1}, u)| < 1/2^k, \forall u \ge j_k \quad (3)$$

Condiţia (3) este vidă pentru $k = 1$.

Să găsim i_n şi j_n încît (1), (2) şi (3) să fie satisfăcute pentru $k = n$.

Şirul $(r_n)_{n \ge 1}$ este Cauchy în $\mathbb{R}$; luînd $\varepsilon = 1/2^{n+1}$, există $i_n \in \mathbb{N}$ astfel încît $i_n > i_{n-1}$ şi

$$|r_s - r_t| < 1/2^{n+1}, \forall s, t \ge i_n \text{ (inegalitate în } \mathbb{R}).$$

Cum $(r(i_n, k))_{k \geq 1}$ e şir Cauchy în $\mathbb{Q}$, $\exists p_n \in \mathbb{N}$ astfel încît

$$|r(i_n, u) - r(i_n, v)| < 1/2^{n+1}, \forall u, v \geq p_n$$

Pe de altă parte, din (1) aplicat pentru $k = n - 1$ şi $s = i_n$, $t = i_{n-1}$, avem $|r_{i_n} - r_{i_{n-1}}| < 1/2^n$ (inegalitate în $\mathbb{R}$), deci (din definiția relației de ordine în $\mathbb{R}$) $\exists q_n$ astfel încît

$$|r(i_n, u) - r(i_{n-1}, u)| < 1/2^n, \forall u \geq q_n.$$

Luînd $j_n = \max(j_{n-1} + 1, p_n, q_n)$, rezultă că (2) şi (3) sînt satisfăcute, cu $k = n$ şi că $j_n > j_{n-1}$. Am construit inductiv şirurile strict crescătoare i_n, j_n, satisfăcînd (1), (2), (3), pentru orice $k \geq 1$.

Notăm $x_n := r(i_n, j_n)$, $\forall n \geq 1$. Să arătăm că $(x_n)_{n \geq 1}$ e şir Cauchy în $\mathbb{Q}$. Pentru orice $n, m \in \mathbb{N}$ cu $n < m$, avem:

$$|x_m - x_n| = |r(i_m, j_m) - r(i_n, j_n)| \leq |r(i_m, j_m) - r(i_n, j_m)| + |r(i_n, j_m) - r(i_n, j_n)| \tag{4}$$

Dar, folosind (3), avem

$$|r(i_m, j_m) - r(i_n, j_m)| = \sum_{k=n+1}^{m} |r(i_k, j_m) - r(i_{k-1}, j_m)| < \sum_{k=n+1}^{m} \frac{1}{2^k} < \frac{1}{2^n}. \tag{4'}$$

Pe de altă parte, $|r(i_n, j_m) - r(i_n, j_n)| < 1/2^n$ pentru că $j_m > j_m$ şi se aplică (2).

Înlocuind în (4), avem:

$$|x_m - x_n| < |r(i_m, j_m) - r(i_n, j_n)| < 1/2^n + 1/2^n = 1/2^{n-1},$$

ceea ce arată că (x_n) este şir Cauchy.

Să arătăm că r_n are limita $x := [(r(i_n, j_n))_{n \geq 1}]$. Fie $\varepsilon > 0$ şi $k \in \mathbb{N}$ astfel încît $1/2^k < \varepsilon/3$. Din (1) avem:

$$|r_s - r_t| < 1/2^{k+1}, \forall s, t \geq i_k \tag{5}$$

Dacă $n \geq i_k$, arătăm că $|r_n - x| < \varepsilon$ (ceea ce va termina demonstrația). Aceasta revine la a proba existența unui N (depinzînd posibil de n) astfel încît $\forall t \geq N$ să avem

$$|r_{nt} - x_t| = |r(n, t) - r(i_t, j_t)| < \varepsilon.$$

Fixăm $q \in \mathbb{N}$ cu $i_q \geq n$. Din (5), $|r_n - r_{i_q}| < 1/2^{k+1}$, deci există un N_0 astfel încît, $\forall t \geq N_0$:

$$|r(n, t) - r(i_q, t)| < \varepsilon/3 \tag{6}$$

Cum r_n e Cauchy, există N_1 astfel încît, $\forall s, t \geq N_1$,

$$|r(n, t) - r(n, s)| < \varepsilon/3 \tag{7}$$

Fie $N := \max(N_0, N_1, i_q)$. Dacă $t \geq N$, avem:

$$|r(n, t) - r(i_t, j_t)| \leq |r(n, t) - r(n, j_t)| + |r(n, j_t) - r(i_q, j_t)| + |r(i_q, j_t) - r(i_t, j_t)| \tag{8}$$

Primul termen din dreapta inegalității (8) e mai mic decît $\varepsilon/3$ din (7). Al doilea termen e mai mic decît $\varepsilon/3$ din (6) (clar, $j_t > t \geq N$). Al treilea termen e mai mic decît $1/2^q$ din (4').

g) Cititorii care au parcurs teoria elementară a convergenței în $\mathbb{R}$ se vor fi întrebat de ce am dat o demonstrație separată pentru *f)*, deşi rezultă din *g)* (vezi Exerciții). Pentru răspuns, vezi construcția de mai jos a *completatului unui corp normat*.

h) Exercițiu. □

Metoda completării prin şiruri Cauchy este folosită şi la ***completatul unui spațiu metric*** oarecare, construcție fundamentală în Analiză şi topologie:

5.3 Definiție. Fie X o mulțime nevidă. O funcție $d : X \times X \to \mathbb{R}$ se numeşte *distanță* (*metrică*) pe X dacă satisface axiomele: i) $\forall x, y \in X$ are loc $d(x, y) = d(y, x) \geq 0$.; ii)$\forall x, y \in X$ are loc: $d(x, y) = 0 \Leftrightarrow x = 0$; iii) $\forall x, y, z \in X$ are loc $d(x, y) \leq d(x, z) + d(z, y)$ (inegalitatea triunghiulară). Un cuplu (X, d), unde d este o distanță pe X, se numeşte *spațiu metric*; elementele lui X se mai numesc şi *puncte* ale lui X.

Pentru orice $x \in X$, *sfera* (*bila*) *deschisă de rază r cu centrul în x* este mulțimea

$$S(x, r) := \{y \in X \mid d(x, y) < r\}.$$

Distanța d defineşte o *topologie* pe X, în care un sistem fundamental de vecinătăți al unui punct $x \in X$ este $\{S(x, r) \mid r \in \mathbb{R}, r > 0\}$ (mulțimea sferelor deschise centrate în x). Altfel spus, o submulțime D a lui X este declarată *deschisă* dacă $\forall x \in D$, $\exists r > 0$ astfel încît $S(x, r) \subseteq D$. Un şir $(x_n)_{n \geq 1}$ este *convergent* la $x \in X$ dacă şi numai dacă $\forall \varepsilon > 0$, $\exists N \in \mathbb{N}$ astfel încît $\forall n > N$ are loc $d(x_n, x) < \varepsilon$. Spațiul metric (X, d) se numeşte *complet* dacă orice şir Cauchy de elemente din X este convergent la un element din X.

Am văzut că $\mathbb{Q}$ este spațiu metric, cu distanța $d(x, y) = |x - y|$, dar nu este complet. Din punct de vedere topologic, construcția lui $\mathbb{R}$ prezentată mai sus este un caz particular al *completării unui spațiu metric*, care, plecînd de la un spațiu metric (X, d), construieşte un spațiu metric *complet* $(\widehat{X}, \widehat{d})$ şi o aplicație injectivă $\varphi : X \to \widehat{X}$, astfel încît $\varphi(X)$ este densă în $\widehat{X}$ şi φ păstrează distanțele. Construcția este asemănătoare cu cea de mai sus, cu deosebirea că nu putem face apel la ideale, nefiind definită nici o structură algebrică pe X. Se foloseşte direct o relație de echivalență "~" definită pe mulțimea $\mathcal{C}$ a şirurilor Cauchy de elemente din X; mulțimea $\mathcal{C}/\sim$ se înzestrează cu o metrică (cum?) şi este spațiul metric complet căutat.

Mai importantă pentru Algebră şi Teoria numerelor este ***completarea unui corp normat.***

5.4 Definiție. Fie K un corp comutativ. O funcție $N : K \to \mathbb{R}$ se numeşte *normă* dacă satisface condițiile:

N1. $\forall x \in K$ are loc $\mathrm{N}(x) \geq 0$.

N2. $\forall x \in K$ are loc $\mathrm{N}(x) = 0 \Leftrightarrow x = 0$.

N3. $\forall x, y \in K$ are loc $\mathrm{N}(x + y) \leq \mathrm{N}(x) + \mathrm{N}(y)$ (inegalitatea triunghiulară).

N4. $\forall x, y \in K$ are loc $\mathrm{N}(x \cdot y) = \mathrm{N}(x) \cdot \mathrm{N}(y)$.

Un cuplu (K, N), unde K este corp şi N o normă pe K se numeşte *corp normat*. Exemple uzuale sînt $(\mathbb{Q}, |\ |)$, $(\mathbb{R}, |\ |)$.

Norma pe K defineşte o metrică $d : K \times K \to \mathbb{R}$ prin relația $d(x, y) := N(x - y)$ (verificați!). Dacă spațiul metric (K, d) *nu* este complet, se poate construi ca mai sus *completatul său* $\widehat{K}$, care e spațiu metric; în plus, se pot defini operații pe $\widehat{K}$ față de care acesta devine corp normat. O abordare mai rapidă reia ideea de a folosi idealul $\mathcal{Z}$ al şirurilor cu limita 0 în inelul $\mathcal{C}$ al şirurilor Cauchy de elemente din K şi construieşte $\widehat{K} := \mathcal{C}/\mathcal{Z}$.

5.5 Exemplu. (**Corpul numerelor** p**-adice**) Fie $p \in \mathbb{Z}$ un număr prim. Dacă $n \in \mathbb{Z}$ şi $\alpha \in \mathbb{N}$, scriem $p^{\alpha} \| n$ dacă $p^{\alpha} | n$ şi $p^{\alpha+1} \nmid n$. Pentru orice $n \in \mathbb{Z}$, $\exists! \alpha \in \mathbb{N}$ astfel încît $p^{\alpha} \| n$. Definim $v_p(n)$, *valuarea p-adică* a lui n, ca fiind unicul numărul natural α astfel încît $p^{\alpha} \| n$. Dacă $r = m/n \in \mathbb{Q}$, cu $m, n \in \mathbb{Z}$, definim[44] $v_p(m/n) := v_p(m) - v_p(n)$. Norma *p-adică* a lui r este

$$|r|_p := p^{-v_p(r)}.$$

Se demonstrează că norma p-adică este o normă pe $\mathbb{Q}$ şi îndeplineşte o proprietate mai tare decît axioma N3 (inegalitatea triunghiulară), anume:

NA: $\forall x, y \in \mathbb{Q}$ are loc $|x + y|_p \le \max(|x|_p, |y|_p)$.

Un corp normat $(K, |\ |)$ care satisface proprietatea NA se numeşte *non-arhimedian* (*sau ultrametric*), deoarece nu satisface *proprietatea lui Arhimede*[45]: $\forall x, y \in K$ cu $x \neq 0$, $\exists n \in \mathbb{N}^*$ astfel încît $|nx| \ge |y|$.

Completatul lui $\mathbb{Q}$ în raport cu norma p-adică se notează cu $\mathbb{Q}_p$ şi se numeşte *corpul numerelor p-adice*. Aceste corpuri joacă un rol important în teoria numerelor.

Aceeaşi idee, a şirurilor Cauchy, apare şi la construcția *completatului unui spațiu liniar normat*. Nu mai intrăm în detalii (vezi de ex. MARINESCU [1983]).

Exerciții

1. a) Fie $a, b \in \mathbb{N}$, $(a, b) = 1$. Folosind algoritmul extins al lui Euclid (vezi Index), arătați că există $\alpha \in a\mathbb{Z}$, $\beta \in b\mathbb{Z}$ astfel încît $1 = \alpha + \beta$. Descrieți un procedeu efectiv de determinare a lui α şi β.

b) Scrieți efectiv izomorfismul canonic $\varphi : \mathbb{Z}_a \times \mathbb{Z}_b \to \mathbb{Z}_{ab}$ dat de lema chineză a resturilor (*Ind.* Aplicați metoda din demonstrația lemei.)

c) Determinați $n \in \mathbb{N}$ astfel încît $n \equiv 7 \pmod{13}$ şi $n \equiv 10 \pmod{18}$.

2. a) Fie p număr natural prim. Arătați că, în inelul de polinoame $\mathbb{Z}_p[X, Y]$, $(X + Y)^p = X^p + Y^p$(*Ind.* Are loc binomul lui Newton, cu coeficienții binomiali calculați mod p.)

3. (*Mica teoremă a lui Fermat*) Fie p număr natural prim şi $a \in \mathbb{N}$. Arătați că $a^p \equiv a \pmod{p}$. (*Ind.* Se poate folosi exercițiul precedent şi o inducție după a. Sau, folosiți teorema lui Lagrange în grupul $(\mathbb{Z}_p^*, \cdot)$)

4. a) Demonstrați că $\mathbb{Z}_{11} \times \mathbb{Z}_{31} \cong \mathbb{Z}_{341}$ şi scrieți efectiv acest izomorfism.

[44] Verificați corectitudinea definiției!
[45] $\mathbb{Q}$ şi $\mathbb{R}$ sînt *corpuri arhimediene*, căci satisfac această proprietate.

b) Calculați 2^{341}(mod 11) şi 2^{341}(mod 31).

c) Demonstrați că $2^{341} \equiv 2$ (mod 341).

d) Este adevărat că, dacă $2^n \equiv 2$ (mod n), atunci n este prim?

5. Demonstrați că în $\mathbb{R}$ (construit cu şiruri Cauchy) orice submulțime nevidă majorată are margine superioară.

6. Fie K un corp comutativ total ordonat în care orice submulțime nevidă majorată are margine superioară. Demonstrați că orice şir Cauchy în K este convergent.

7. (Construcția lui Dedekind a lui $\mathbb{R}$ prin tăieturi în $\mathbb{Q}$) Se numeşte *tăietură* în $\mathbb{Q}$ o pereche (A, B) de submulțimi ale lui $\mathbb{Q}$ cu proprietățile: i) $A \neq \varnothing$, $B \neq \varnothing$; ii) $A \bigcup B = \mathbb{Q}$; iii) $\forall a \in A$, $\forall b \in B$ are loc $a < b$; iv) A nu are cel mai mare element.

Fie $T(\mathbb{Q}) := \{(A, B) \mid (A, B)$ tăietură în $\mathbb{Q}\}$. Demonstrați că:

a) Dacă (A, B) este tăietură în $\mathbb{Q}$, atunci $A \bigcap B = \varnothing$ şi $B = \mathbb{Q} \setminus A$.

b) Definind relația " $\leq$ " pe $T(\mathbb{Q})$ prin $(A, B) \leq (C, D) \Leftrightarrow A \subseteq C$ ($\Leftrightarrow D \subseteq B$), se obține o relație de ordine totală pe $T(\mathbb{Q})$.

c) Aplicația $\varphi : \mathbb{Q} \to T(\mathbb{Q})$, $\varphi(x) = (L_x, R_x)$, cu $L_x = \{y \in \mathbb{Q} \mid y < x\}$ şi $R_x = \{y \in \mathbb{Q} \mid y \geq x\}$, este injectivă şi crescătoare (deci x poate fi identificat cu $\varphi(x) \in T(\mathbb{Q})$, iar $\mathbb{Q}$ cu $\varphi(\mathbb{Q})$).

d) Orice submulțime $(A_i, B_i)_{i \in I}$ a lui $T(\mathbb{Q})$ care este majorată în $T(\mathbb{Q})$ are margine superioară, anume $(\bigcup_{i \in I} A_i, \bigcap_{i \in I} B_i) \in T(\mathbb{Q})$.

e) Definind: $(A, B) + (C, D) := (A + C, B + D)$, $\forall (A, B), (C, D) \in T(\mathbb{Q})$, (unde $A + C = \{a + c \mid a \in A,\ c \in C\}$), se obține o lege de compoziție pe $T(\mathbb{Q})$; $(T(\mathbb{Q}), +)$ este grup abelian, iar $\varphi : \mathbb{Q} \to T(\mathbb{Q})$ definit mai sus este morfism de grupuri.

f) Fie $\alpha = (A, B)$, $\beta = (C, D) \in T(\mathbb{Q})$. Definim "$\cdot$": $T(\mathbb{Q}) \times T(\mathbb{Q}) \to T(\mathbb{Q})$ prin:

$$\alpha \cdot \beta = \begin{cases} (AC, BD) & \text{dacă } \alpha, \beta \geq 0 \\ |\alpha| \cdot |\beta| & \text{dacă } \alpha, \beta < 0 \\ -|\alpha| \cdot |\beta| & \text{în celelalte cazuri} \end{cases}$$

(unde $A \cdot C = \{a \cdot c \mid a \in A,\ c \in C\}$ şi $|\ |$ este funcția modul pe K). Atunci $(T(\mathbb{Q}), +, \cdot, \leq)$ este corp ordonat şi $\varphi : \mathbb{Q} \to T(\mathbb{Q})$ este morfism de corpuri.

8. Verificați afirmațiile nedemonstrate de la exemplul II.5.5.

III. Polinoame, corpul complex şi extinderi de corpuri

Conceptul de *polinom* (cu coeficienţi într-un inel dat, adesea $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) joacă un rol central în matematică şi este legat de noţiunea de *funcţie polinomială*, cu care este de altfel confundat adesea. Această confuzie este inofensivă în cazul inelelor integre infinite, dar nu şi în cazul inelelor care nu sînt integre sau infinite; mai mult, conceperea polinoamelor într-o manieră structurală (ca elemente ale unui nou inel construit plecînd de la un inel dat) are avantajul de a conduce la construcţii importante şi nebanale. În plus, se poate generaliza construcţia riguroasă a inelului clasic de polinoame la inele monoidale, grupale…

Intuitiv, un *polinom* (cu coeficienţi într-un inel dat, să zicem *corpul numerelor reale* $\mathbb{R}$) este o „expresie" de forma

$$f = a_0 + a_1 X + \ldots + a_n X^n \qquad (1)$$

în care apare o „variabilă" sau „nedeterminată" X, iar $a_0, a_1, \ldots, a_n$ sînt „coeficienţii polinomului": nişte elemente fixate ale inelului dat (în cazul nostru numere reale fixate).

Cea mai la îndemînă interpretare riguroasă a acestui obiect matematic este cea a *funcţiei* $\widetilde{f} : \mathbb{R} \to \mathbb{R}$, $\widetilde{f}(x) = a_0 + a_1 x + \ldots + a_n x^n$, $\forall x \in \mathbb{R}$. Să considerăm însă inelul $\mathbb{Z}_3$ al claselor de resturi modulo 3 şi polinoamele $f = X^3$ şi $g = X$ cu coeficienţi în $\mathbb{Z}_3$. Se observă că funcţiile $\widetilde{f} : \mathbb{Z}_3 \to \mathbb{Z}_3$ şi $\widetilde{g} : \mathbb{Z}_3 \to \mathbb{Z}_3$ date de $\widetilde{f}(x) = x^3$ şi $\widetilde{g}(x) = x$ sînt egale! Polinoamele f şi g *nu* sînt totuşi identice.

O soluţie ar fi să definim un polinom cu coeficienţi într-un inel dat R ca o „sumă formală" de tipul (1), în care $a_0, a_1, \ldots, a_n \in R$ sînt „coeficienţii polinomului", iar X are un rol special, de „nedeterminată", putînd fi înlocuită cu *orice element al lui R*. Aceste „sume formale" se adună şi înmulţesc după regulile binecunoscute. Mulţimea acestor „sume formale de tipul (1)" cu coeficienţi în R devine atunci un *inel*, notat $R[X]$.

Dar, în aplicaţii, nedeterminata X este adesea înlocuită cu un element dintr-un inel S *diferit* de inelul iniţial R. De exemplu, în cazul polinoamelor cu coeficienţi în $\mathbb{R}$, X poate fi înlocuită cu un *număr complex* sau cu o *matrice pătratică* cu elemente numere reale. Mai general, se pot da nedeterminatei valori alese într-o R-*algebră* (noţiune detaliată mai jos). Procedeul de „înlocuire a nedeterminatei" sau de „evaluare a unui polinom într-un punct", asociază la fiecare polinom f şi fiecărui $a \in A$ (unde A este o R-algebră) un element $f(a) \in A$ şi trebuie să satisfacă regulile:

$$(f + g)(a) = f(a) + g(a);\ (f \cdot g)(a) = f(a) \cdot g(a), \text{ pentru orice polinoame } f \text{ şi } g \in R[X]$$

Este util să fixăm $a \in A$ şi să considerăm „evaluarea în a” ca o funcţie $v_a : R[X] \to A$, $v_a(f) = f(a)$. Proprietăţile de mai sus revin atunci la a spune că v_a este *morfism de inele*.

Aceste idei intuitive despre polinoame se exprimă riguros şi formal în secţiunea următoare, unde, pornind de la un inel R şi un monoid G, se construieşte R-*algebra monoidală* $R[G]$. În cazurile particulare $G = (\mathbb{N}, +)$ şi $G = (\mathbb{N}^n, +)$ se regăsesc algebrele clasice de polinoame $R[X]$, respectiv $R[X_1,\ldots, X_n]$.

Cititorii care sînt familiarizaţi cu noţiunea de R-algebră şi inelele clasice de polinoame şi nu sînt interesaţi de algebre monoidale pot trece direct la **III.2**, construcţia lui $\mathbb{C}$.

III.1 Algebre. Algebre monoidale şi algebre polinomiale

Fie $(R, +, \cdot)$ un inel *comutativ unitar*, cu elementul unitate notat cu 1, fixat pe tot cuprinsul acestui paragraf. Începem cu unele definiţii referitoare la R-algebre.

1.1 Definiţie. Se numeşte *R-algebră* un inel $(A, +, \cdot)$ (nu neapărat asociativ sau unitar), înzestrat cu o *operaţie externă* "$\cdot$" $: R \times A \to A$, $(r, a) \mapsto ra$, care îi conferă o structură de R-modul[46], astfel încît să aibă loc condiţiile:

$$r(ab) = (ra)b = a(rb),\ \forall r \in R,\ \forall a, b \in A.$$

R-algebra A se numeşte *asociativă* (respectiv *unitară, comutativă*) dacă inelul A are proprietatea corespunzătoare. Notăm cu $\mathrm{Cen}(A) := \{a \in A \mid ab = ba,\ \forall b \in A\}$ *centrul* lui A, adică subinelul format din elementele care comută cu orice element al lui A.

Pentru R-algebrele *asociative şi unitare* există următoarea caracterizare (care poate fi luată drept *definiţie* a noţiunii de R-algebră):

1.2 Propoziţie. *a) Fie A o R-algebră asociativă şi unitară şi e elementul său unitate. Atunci aplicaţia $\alpha : R \to A$ definită de $\alpha(r) := re$, $\forall r \in R$, este un morfism unitar de inele cu proprietatea că $\alpha(r)a = a\alpha(r)$, $\forall r \in R$, $\forall a \in A$ (adică $\alpha(R) \subseteq \mathrm{Cen}(A)$).*

b) Reciproc, dacă A este un inel asociativ şi unitar, iar $\alpha : R \to A$ este un morfism unitar de inele cu $\alpha(R) \subseteq \mathrm{Cen}(A)$, atunci A devine o R-algebră definind operaţia de R-modul prin

$$ra := \alpha(r)a,\ \forall r \in R,\ \forall a \in A.$$

Demonstraţie. *a)* Dacă $r, s \in R$, atunci, folosind definiţia R-algebrei, avem:

$$\alpha(r + s) = (r + s)e = re + se = \alpha(r) + \alpha(s)$$

$$\alpha(r)\alpha(s) = (re)(se) = r(e(se)) = r(se) = (rs)e = \alpha(rs).$$

---

[46] Reamintim că axiomele din definiţia unui R-modul M sînt exact cele ale unui K-spaţiu liniar M (înlocuind peste tot corpul K cu inelul R).

Avem $\alpha(1) = 1e = e$ (căci A este R-modul). Astfel, α este morfism unitar de inele. Dacă $r \in R$, $a \in A$, $\alpha(r)a = (re)a = r(ea) = ra = r(ae) = a(re) = a\alpha(r)$. □

Morfismul $\alpha : R \to A$ dat de teorema de mai sus se numeşte *morfismul structural* al R-algebrei asociative şi unitare A. Evident, un inel A poate avea mai multe structuri de R-algebră (depinzînd de morfismul structural, respectiv de operația externă "$\cdot$" : $R \times A \to A$).

1.3 Exemple. a) Inelul de matrice pătratice $M_n(R)$ este o R-algebră asociativă şi unitară (necomutativă dacă $n \geq 2$). Morfismul structural asociază lui $r \in R$ matricea cu r pe diagonala principală şi 0 în rest.

b) Inelul de polinoame $R[X]$ este o R-algebră comutativă. Dacă $K \subseteq L$ este o extindere de corpuri, L este o K-algebră. Care sînt morfismele structurale (echivalent, care este structura de modul) pentru aceste exemple?

1.4 Definiție. Fie A şi B două R-algebre. Un morfism de inele $\varphi : A \to B$ care este şi morfism de R-module se numeşte *morfism de R-algebre*. Mai precis, φ este morfism de R-algebre dacă şi numai dacă, $\forall r \in R$, $\forall a, b \in A$, au loc:

$$\varphi(a + b) = \varphi(a) + \varphi(b);\ \ \varphi(ab) = \varphi(a)\varphi(b) \text{ (φ este morfism de inele);}$$

$$\varphi(ra) = r\varphi(a) \text{ (φ este şi morfism de R-module).}$$

Dacă A şi B sînt *asociative* şi *unitare*, iar α, respectiv β sînt morfismele structurale, un morfism *unitar* de inele $\varphi : A \to B$ este morfism de R-algebre dacă şi numai dacă $\varphi \circ \alpha = \beta$ (Verificați!).

În continuare, *prin R-algebră vom înțelege o R-algebră unitară şi asociativă.*

1.5 Definiție. O submulțime C a R-algebrei A se numeşte *R-subalgebră* a lui A dacă C este subinel în A şi $\forall r \in R$, $\forall a \in C$, rezultă $ra \in C$ (adică C este şi R-submodul în A).

Intersecția unei familii de subalgebre ale lui A este tot o subalgebră a lui A (demonstrați!). Astfel, pentru o submulțime oarecare S a lui A, se poate defini *subalgebra generată de S*: este *intersecția tuturor subalgebrelor lui A care includ S*.

1.6 Exercițiu. a) Fie A o R-algebră unitară şi $x \in A$. Atunci subalgebra generată de $\{x\}$ (notată cu $R[x]$) este mulțimea „expresiilor polinomiale în x cu coeficienți în R", adică:

$$R[x] = \{a_0 + a_1x + \ldots + a_nx^n \mid n \in \mathbb{N}, a_0, a_1, \ldots, a_n \in R\}.$$

b) Fie A o R-algebră unitară şi $S \subseteq \mathrm{Cen}(A)$. Atunci subalgebra generată de S (notată cu $R[S]$) este mulțimea „expresiilor polinomiale în elementele lui S, cu coeficienți în R", adică:

$$R[S] = \left\{ \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{i_1\ldots i_n} s_1^{i_1}\ldots s_n^{i_n} \;\middle|\; a_{i_1\ldots i_n} \in R, s_1,\ldots s_n \in S \right\},$$

unde sumele sînt finite (doar un număr finit dintre $a_{i_1\ldots i_n}$ sînt nenuli). Acest rezultat dă forma subalgebrei generate de orice submulțime S a unei R-algebre *comutative* şi unitare.

Pentru R-algebre şi morfisme de R-algebre au loc proprietăţile uzuale de la inele şi morfisme de inele. Astfel, au loc următoarele proprietăţi şi construcţii, întru totul analoage celor de la inele (demonstraţi!):

a) *Dacă* $\varphi: A \to B$ *este morfism de R-algebre*, atunci $\varphi(A)$ *este o subalgebră a lui B*.

b) Un ideal bilateral I al inelului A se mai numeşte *ideal* al R-algebrei A. *Dacă I este ideal bilateral al R-algebrei A de morfism structural* α, *atunci inelul factor* A/I *este o R-algebră, de morfism structural* $\pi \circ \alpha$, *unde* $\pi: A \to A/I$ *este proiecţia canonică. Această algebră se numeşte algebra factor a lui A relativ la idealul I.*

c) *Dacă* $\varphi: A \to B$ *este un morfism de R-algebre, atunci* $\operatorname{Ker}\varphi = \{a \in A \mid \varphi(a) = 0\}$ *este ideal al lui A şi are loc teorema fundamentală de izomorfism:*

$$\frac{A}{\operatorname{Ker}\varphi} \cong \operatorname{Im}\varphi \ \ (\textit{izomorfism de R-algebre}).$$

Construcţia clasică a inelului de polinoame $R[X]$ cu coeficienţi în inelul comutativ R (în care un *polinom* este definit ca *un şir de elemente din R, şir în care un număr finit de termeni sînt nenuli*) este predată în liceu şi *o presupunem cunoscută*. Vom prezenta o generalizare a acestei construcţii, care permite între altele obţinerea directă a inelului de polinoame de mai multe nedeterminate şi scoate în evidenţă rolul esenţial al *morfismului de evaluare*.

Fiind dat un monoid $(G, \cdot)$ şi un inel comutativ R, vom construi **algebra monoidală** $R[G]$ peste inelul R. Se obţin drept cazuri particulare inelele de polinoame de una, două, sau o mulţime oarecare de nedeterminate.

Ideea ce stă la baza construcţiei este următoarea: *fiind date inelul comutativ R şi monoidul* $(G, \cdot)$, *pe* $R^{(G)}$ *(R-modulul liber peste mulţimea G) se defineşte o operaţie de înmulţire asociativă şi distributivă faţă de adunarea din* $R^{(G)}$, *care pentru elementele lui G să coincidă cu înmulţirea din G.* Orice element din $R^{(G)}$ se scrie în mod unic ca o sumă finită de forma

$$\sum_{g \in G} a_g g \text{ , (cu } a_g \in R, \forall g \in G).$$

Altfel spus, elementele lui G sînt văzute ca elementele unei baze în R-modulul liber $R^{(G)}$. *Produsul* dintre $g, h \in G$ (văzute ca elemente în baza lui $R^{(G)}$) este gh (văzut tot ca element în baza lui $R^{(G)}$); acest produs se extinde la orice element al lui $R^{(G)}$ de forma de mai sus, astfel încît să fie respectată distributivitatea înmulţirii faţă de adunare. *Detalierea* acestei idei este făcută în continuare.

Fie deci $(G, \cdot)$ un monoid (adică G este o mulţime nevidă înzestrată cu o operaţie „·", asociativă şi cu element neutru e). Construim mai întîi *mulţimea suport* pe care o vom structura cu operaţii.

Definim *suportul* unei aplicaţii $\varphi: G \to R$ ca fiind mulţimea $\operatorname{supp}(\varphi) := \{g \in G \mid \varphi(g) \neq 0\}$. *Notăm* $R[G] := \{\varphi: G \to R \mid \operatorname{supp}(\varphi) \text{ este finit}\}$.

O funcţie din $R[G]$ se numeşte *funcţie de suport finit*.[47] Pe $R[G]$ definim *adunarea* şi *înmulţirea*: $\forall \varphi, \psi \in R[G]$, $\forall g \in G$, punem

$$(\varphi+\psi)(g) := \varphi(g)+\psi(g)$$
$$(\varphi\cdot\psi)(g) := \sum_{\substack{(u,v)\in G\times G\\ uv=g}} \varphi(u)\psi(v).$$

Prima egalitate defineşte cu claritate $\varphi+\psi$ ca funcţie de la G la R. Trebuie arătat că şi $\varphi\psi$ este corect definită, adică suma din definiţia lui $\varphi\cdot\psi$ are un număr finit de termeni nenuli. Într-adevăr, mulţimea perechilor $(u,v) \in G\times G$ cu proprietatea că $\varphi(u)\psi(v) \neq 0$ este inclusă în $\text{supp}(\varphi)\times\text{supp}(\psi)$, care este finită.

1.7 Observaţie. Definiţia adunării $\varphi+\psi$ este naturală. Să explicăm de ce s-a definit ca mai sus *înmulţirea* $\varphi\cdot\psi$. În cazul clasic, în care $(G, \cdot)$ este $(\mathbb{N}, +)$, fie $\varphi = (a_0, a_1,\ldots, a_n, \ldots)$, $\psi = (b_0, b_1,\ldots, b_n, \ldots)$, adică $\varphi(i) = a_i$ …etc. Atunci $\varphi\cdot\psi$ este definit ca $(c_0, c_1,\ldots, c_n, \ldots)$, unde:

$$c_k = a_0b_k + a_1b_{k-1} + \ldots + a_kb_0 = \sum_{\substack{(u,v)\in\mathbb{N}\times\mathbb{N}\\ u+v=k}} a_ub_v = \sum_{\substack{(u,v)\in\mathbb{N}\times\mathbb{N}\\ u+v=k}} \varphi(u)\psi(v)$$

Trebuie să arătăm că $\varphi+\psi$ şi $\varphi\psi$ *sînt funcţii de suport finit*. Se observă că $\text{supp}(\varphi+\psi) \subseteq \text{supp}(\varphi) \bigcup \text{supp}(\psi)$, care e finită. Pentru $\varphi\psi$, dacă $g \in G \setminus \{uv \mid u \in \text{supp}(\varphi) \text{ şi } v \in \text{supp}(\psi)\}$, atunci $(\varphi\psi)(g)$ este 0, căci toţi termenii din suma din definiţie sînt nuli. Deci $\text{supp}(\varphi\psi)$ este inclus în $\{uv \mid u \in \text{supp}(\varphi) \text{ şi } v \in \text{supp}(\psi)\}$, care este finită.

Aşadar, „+” şi „ · ” *sînt corect definite şi sînt legi de compoziţie internă pe* $R[G]$. Se poate defini şi o *operaţie externă* „·” : $R \times R[G] \to R[G]$, prin

$$(r\varphi)(g) := r\varphi(g),\ \forall r \in R,\ \forall \varphi \in R[G],\ \forall g \in G.$$

În raport cu această operaţie, $R[G]$ *devine R-modul*, care este (izomorf cu) R-modulul liber de bază G (dacă se face abstracţie de operaţia de înmulţire în $R[G]$).

1.8 Propoziţie. $(R[G], +, \cdot)$ *este inel asociativ unitar.*

Demonstraţie. Probăm asociativitatea înmulţirii. Fie $\varphi, \psi, \eta \in R[G]$ şi $g \in G$.

$$((\varphi\psi)\eta)(g) = \sum_{\substack{(u,v)\in G^2\\ uv=g}} (\varphi\psi)(u)\eta(v) = \sum_{\substack{(u,v)\in G^2\\ uv=g}} \left(\sum_{\substack{(s,t)\in G^2\\ st=u}} \varphi(s)\psi(t) \right)\eta(v) = \sum_{\substack{(s,t,v)\in G^3\\ stv=g}} \varphi(s)\psi(t)\eta(v).$$

Calculînd $(\varphi(\psi\eta))(g)$, se obţine acelaşi lucru, deci $(\varphi\psi)\eta = \varphi(\psi\eta)$.

Existenţa elementelor neutre pentru adunare şi înmulţire este demonstrată mai jos. Verificarea celorlalte axiome este propusă ca exerciţiu. □

---

[47] A se observa analogia cu cazul clasic, în care $(G, \cdot)$ este $(\mathbb{N}, +)$. Un „şir de elemente din R cu un număr finit de termeni nenuli” este de fapt o funcţie $\varphi : \mathbb{N} \to R$, de suport finit.

1.9 Observaţie. Din construcţie, rezultă că $R[G]$ este izomorf cu R-modulul liber de bază G. Putem scrie elementele lui $R[G]$ ca sume „formale" finite de forma $\sum_{g\in G} a_g g$, cu $(a_g)_{g\in G}$ o familie de suport finit de elemente din R, indexată după elementele lui G. Se „identifică" $a \in R$ cu „suma" cu un termen $a\cdot e$; la fel, identificăm $g \in G$ cu $1\cdot g$. Aceste identificări revin de fapt la a defini două morfisme injective $i : R \to R[G]$ şi $j : G \to R[G]$ (vezi propoziţia de mai jos). Adunarea se face după regula $\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g)g$, iar înmulţirea satisface distributivitatea la stînga şi la dreapta faţă de adunare şi regula $(1\cdot g)\cdot(1\cdot h) = 1\cdot(gh)$. Avem :

$$\left(\sum_{g\in G} a_g g\right)\cdot\left(\sum_{g\in G} b_g g\right) = \sum_{g\in G}\left(\sum_{uv=g}(a_u b_v)\right)g .$$

Astfel, $R[G]$ satisface condiţiile de la începutul acestui paragraf. Orice element al lui $R[G]$ se scrie în mod unic sub forma $\sum_{g\in G} a_g g$, subînţelegîndu-se că este vorba de sume finite. În particular, $\sum_{g\in G} a_g g = 0 \Leftrightarrow a_g = 0$, $\forall g \in G$.

Să facem legătura cu inelele de polinoame clasice şi să arătăm că această construcţie satisface cerinţele de la începutul paragrafului. Considerăm următoarele elemente din $R[G]$:

$\forall g \in G$, definim $\eta_g : G \to R$ prin $\eta_g(h) = \begin{cases} 0, \text{dacă } h \neq g \\ 1, \text{dacă } h = g \end{cases}$, $\forall h \in G$;

$\forall r \in R$, definim $\psi_r : G \to R$ prin $\psi_r(h) = \begin{cases} 0, \text{dacă } h \neq e \\ r, \text{dacă } h = e \end{cases}$, $\forall h \in G$.

Este evident că $\eta_g, \psi_r \in R[G]$, $\forall g \in G, \forall r \in R$. Au loc următoarele proprietăţi:

1.10 Propoziţie. *a) Aplicaţia* $i : R \to R[G]$*, dată prin* $i(r) = \psi_r$*,* $\forall r \in R$*, este un morfism injectiv de inele. În plus,* $\operatorname{Im} i \subseteq R[G]$ *(adică* $R[G]$ *este o R-algebră de morfism structural i). De aceea, vom scrie r în loc de* ψ_r *(identificînd pe* $r \in R$ *cu imaginea sa* $\psi_r \in R[G]$*).*

b) Aplicaţia $j : G \to (R[G], \cdot)$*,* $j(g) = \eta_g$*,* $\forall g \in G$*, este un morfism injectiv de monoizi. Vom scrie g în loc de* η_g *(identificînd pe* $g \in G$ *cu imaginea sa* $\eta_g \in R[G]$*).*

c) Pentru orice $g, h \in G$ *şi* $r \in R$*, avem* $(\psi_r\cdot \eta_g)(h) = \begin{cases} 0, \text{dacă } h \neq g \\ r, \text{dacă } h = g \end{cases}$.

d) Fie $\varphi \in R[G]$*. Notăm* $\varphi(g)$ *cu* a_g*,* $\forall g \in G$*. Atunci* φ *se scrie sub forma unei sume finite:*

$$\varphi = \sum_{g\in \operatorname{supp}(\varphi)} a_g g ,$$

unde am identificat pe η_g *cu g şi pe* ψ_{a_g} *cu* $a_g = \varphi(g)$*,* $\forall g \in G$*.*

Scrierea lui φ *este unică: dacă* $\sum_{g\in G} a_g g = \sum_{g\in G} b_g g$*, pentru două aplicaţii de suport finit* $g \mapsto a_g$ *şi* $g \mapsto b_g$ *de la G la R, atunci* $a_g = b_g$*,* $\forall g \in G$*.*

e) Elementul neutru pentru adunare este ψ_0 *(scris ca sumă de tipul* $\sum_{g\in G} a_g g$ *sub forma sumei cu un termen* $0e$*). Elementul neutru la înmulţire este* $\eta_e = 1e$*.*

Demonstrație. *a)* Evident, $\psi_{r+s} = \psi_r + \psi_s$, $\forall r, s \in R$. Calculînd $\psi_r \cdot \psi_s$, obținem $\psi_r \cdot \psi_s(g) = \sum_{uv=g} \psi_r(u)\psi_s(v)$. Dacă $g \neq e$, atunci, pentru orice cuplu (u, v) cu proprietatea că $uv = g$, avem că $u \neq e$ sau $v \neq e$, deci $\psi_r(u)\psi_s(v) = 0$. Aşadar, dacă $g \neq e$, atunci $\psi_r \cdot \psi_s(g) = 0$. La fel se observă că $(\psi_r \cdot \psi_s)(e) = \psi_r(e) \cdot \psi_s(e) = rs$. În concluzie, avem $\psi_r \cdot \psi_s = \psi_{rs}$. Injectivitatea este clară.

b) Arătăm că $\eta_g \eta_h = \eta_{gh}$, $\forall g, h \in G$. Pentru $\forall x \in G$, $x \neq gh$, avem $(\eta_g \eta_h)(x) = \sum_{uv=x} \eta_g(u)\eta_h(v) = 0$, căci din $uv = x \neq gh$ rezultă că $u \neq g$ sau $v \neq h$. Pe de altă parte, $(\eta_g \eta_h)(gh) = 1$ (verificare uşoară).

d) Avem, $\forall h \in G$,

$$\left(\sum_{g\in \operatorname{supp}\varphi} a_g g\right)(h) = \sum_{g\in \operatorname{supp}(\varphi)} \left(\psi_{\varphi(g)}\eta_g\right)(h) = \begin{cases} 0, \text{dacă } h \notin \operatorname{supp}(\varphi) \\ \varphi(h), \text{dacă } h \in \operatorname{supp}(\varphi) \end{cases} = \varphi(h).$$

Am folosit în ultima egalitate faptul că $\left(\psi_{\varphi(g)}\eta_g\right)(h) = \begin{cases} 0, \text{dacă } h \neq g \\ \varphi(g), \text{dacă } h = g \end{cases}$, după punctul *c)*.

Unicitatea rezultă din $\left(\sum_{g\in G} a_g g\right)(h) = a_h$, $\forall h \in G$.

e) Demonstrăm că η_e este unitatea inelului $R[G]$. Pentru orice $g \in G$, avem $\eta_g \eta_e = \eta_{ge} = \eta_g = \eta_e \eta_g$ (am aplicat *c)*). Cazul general rezultă folosind *d)* şi distributivitatea. □

Dacă G este monoid comutativ, atunci şi $R[G]$ este inel comutativ. Dacă G nu este comutativ, atunci nici $R[G]$ nu este comutativ (vezi *b)* de mai sus).

Algebrele polinomiale clasice

1. Pentru $(G, \cdot) = (\mathbb{N}, +)$ se obține construcția uzuală a *R-algebrei de polinoame într-o nedeterminată*[48] *cu coeficienți în R*. Într-adevăr, $R[\mathbb{N}]$ este format din funcțiile $\varphi : \mathbb{N} \to R$ de suport finit (adică şiruri finite de elemente din R). Notînd $\varphi(i) =: a_i$, $\forall i \in \mathbb{N}$, forma generală a unui element f din $R[\mathbb{N}]$ este $f = \sum_{i\in \mathbf{N}} a_i \eta_i$. Ținînd cont că $\eta_i \eta_j = \eta_{i+j}$, pentru orice $i, j \in \mathbb{N}$, avem că $\eta_i = (\eta_1)^i$, $\forall i \in \mathbb{N}$. Notînd η_1 cu X, se obține scrierea uzuală $f = \sum_{i\in\mathbb{N}} a_i X^i$(sumă finită). $R[\mathbb{N}]$ se notează de obicei cu $R[X]$.

2. Considerînd monoidul comutativ $(\mathbb{N}^n, +)$ (pentru $n \in \mathbb{N}^*$ fixat), unde adunarea este definită pe componente, se obține construcția R-algebrei $R[\mathbb{N}^n]$, numită *R-algebra de polinoame în n nedeterminate*. Un element din $R[\mathbb{N}^n]$ se numeşte *polinom* (în n nedeterminate). Pentru a face legătura cu scrierea clasică a polinoamelor, fie $e_i := (0,\ldots,1,\ldots,0) \in \mathbb{N}^n$ (1 pe locul i, 0 în rest), pentru fiecare $i \in \{1, \ldots, n\}$. Se vede uşor că orice element din $\mathbb{N}^n$ se scrie în mod unic – pînă la o ordine a termenilor – ca o sumă de e_i (cu alte

[48] Se mai foloseşte terminologia „necunoscută" sau „variabilă" în loc de „nedeterminată".

cuvinte, e_i generează monoidul $\mathbb{N}^n$). Notăm elementul η_{e_i} cu X_i şi îl numim *nedeterminată*. Un produs de nedeterminate (de forma $X_1^{i_1}\ldots X_n^{i_n}$) se numeşte *term*. Orice polinom g din $R[\mathbb{N}^n]$ se scrie în mod unic sub forma unei sume finite:

$$g = \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{i_1\ldots i_n} X_1^{i_1}\ldots X_n^{i_n},$$

unde $\left(a_{i_1\ldots i_n}\right)_{(i_1,\ldots,i_n)\in\mathbb{N}^n}$ este o familie *de suport finit* de elemente din R. Deci g este o combinaţie liniară cu coeficienţi în R de termi. Orice termen al sumei din membrul drept (de forma $a_{i_1\ldots i_n} X_1^{i_1}\ldots X_n^{i_n}$, cu $a_{i_1\ldots i_n}\in R$, nenul) se numeşte *monom* al lui g.

Invităm cititorul să verifice afirmaţiile nedemonstrate de mai sus. $R[\mathbb{N}^n]$ se notează de obicei cu $R[X_1,\ldots, X_n]$.

3. *Inelul de polinoame de S nedeterminate*, unde S este o mulţime nevidă oarecare. Se consideră mulţimea $\mathbb{N}^{(S)}$ a funcţiilor de suport finit definite pe S cu valori în $\mathbb{N}$. Interpretăm elementele lui $\mathbb{N}^{(S)}$ ca „multiindici” şi le notăm cu $\mathbf{i}$, $\mathbf{j}$,… . Înzestrăm $\mathbb{N}^{(S)}$ cu o operaţie notată aditiv: dacă $\mathbf{i}, \mathbf{j}\in\mathbb{N}^{(S)}$, punem $(\mathbf{i}+\mathbf{j})(s) = \mathbf{i}(s)+\mathbf{j}(s)$, $\forall s\in S$. Se vede imediat că se obţine o structură de monoid comutativ. Inelul $R[\mathbb{N}^{(S)}]$ se numeşte *inelul de polinoame de S nedeterminate cu coeficienţi în R*. Pentru orice $s\in S$, considerăm funcţia $\mathbf{e}_s\in\mathbb{N}^{(S)}$, dată prin $\mathbf{e}_s(t)=\begin{cases}0, \text{dacă } s=t\\ 1, \text{dacă } s\neq t\end{cases}$, $\forall t\in S$ şi notăm cu X_s elementul $\eta_{\mathbf{e}_s}\in R[\mathbb{N}^{(S)}]$. Orice element $\mathbf{i}$ din $\mathbb{N}^{(S)}$ se scrie în mod unic sub forma $\mathbf{i} = \sum_{s\in S} m_s\mathbf{e}_s$, unde $(m_s)_{s\in S}$ este o familie de suport finit de numere naturale[49] indexată după S. Aşadar, $\eta_{\mathbf{i}} = \prod_{s\in\mathrm{supp}(\mathbf{i})} X_s^{m_s}$. În consecinţă, un polinom oarecare f din $R[\mathbb{N}^{(S)}]$ se scrie sub forma $f=\sum_{\mathbf{i}\in F} a_{\mathbf{i}}\eta_{\mathbf{i}}$, cu F o submulţime finită a lui $\mathbb{N}^{(S)}$; dacă notăm $\bigcup_{\mathbf{i}\in F}\mathrm{supp}(\mathbf{i})$ cu $\{s_1, \ldots, s_n\}$ (este o submulţime finită a lui S), atunci avem o scriere

$$f=\sum_{(m_1,\ldots,m_n)\in\mathbb{N}^n} a_{m_1\ldots m_n} X_{s_1}^{m_1}\ldots X_{s_n}^{m_n},$$

unde suma este finită, adică familia $\left(a_{m_1\ldots m_n}\right)_{(m_1,\ldots,m_n)\in\mathbb{N}^n}$ este de suport finit.

Se observă că *orice polinom de S nedeterminate este polinom de un număr finit de nedeterminate din S*. Inelul $R[\mathbb{N}^{(S)}]$ se notează cu $R[(X_s)_{s\in S}]$ sau $R[X_s]_{s\in S}$ sau $R[X; S]$.

Teorema care urmează este de primă importanţă şi generalizează într-un cadru abstract procedura de „înlocuire a nedeterminatei (nedeterminatelor) cu o valoare (valori)dintr-o R-algebră”.

[49] Evident, înmulţirea dintre $m\in\mathbb{N}$ şi $\mathbf{i}\in R[\mathbb{N}^{(S)}]$ este dată de $(m\mathbf{i})(s) := m\cdot\mathbf{i}(s)$, $\forall s\in S$.

1.11 Teoremă. (Proprietatea de universalitate a algebrei monoidale) *Fie R un inel comutativ, $(G, \cdot)$ un monoid şi $i : R \to R[G]$, $j : G \to R[G]$ aplicaţiile canonice definite la* **1.10**. *Tripletul format din algebra monoidală $R[G]$ împreună cu aplicaţiile i şi j are următoarea* proprietate de universalitate*: pentru orice R-algebră T de morfism structural $\alpha : R \to T$ şi orice morfism de monoizi $\beta : G \to (T, \cdot)$, există un unic morfism de R-algebre $\varphi : R[G] \to T$ astfel încît $\varphi \circ i = \alpha$ şi $\varphi \circ j = \beta$:*

$$\begin{array}{ccc} G & \xrightarrow{j} & R[G] \\ & \searrow^{\beta} & \vdots\ \varphi \\ & & T \end{array}$$

Demonstraţie. Presupunem că φ este un morfism cu proprietăţile din enunţ. Aşadar, $\varphi(r) = \alpha(r)$, $\forall r \in R$ şi $\varphi(g) = \beta(g)$, $\forall g \in G$. Dacă $\sum_{g\in G} a_g g$ este un element oarecare din $R[G]$, atunci $\varphi\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} \varphi(a_g)\varphi(g) = \sum_{g\in G} \alpha(a_g)\beta(g)$, ceea ce arată că φ este unic determinat de α şi β. Un calcul direct arată că φ dat de egalitatea de mai sus este morfism de inele şi satisface condiţiile cerute. □

1.12 Observaţie. Proprietatea de universalitate a algebrei monoidale *determină această algebră pînă la un (unic) izomorfism*: dacă tripletul (A, γ, δ) (cu A o R-algebră de morfism structural $\gamma : R \to A$ şi cu $\delta : G \to (A, \cdot)$ un morfism de monoizi) satisface aceeaşi proprietate de universalitate ca tripletul $(R[G], i, j)$, atunci există un unic izomorfism de R-algebre $\varphi : R[G] \to A$ astfel încît $\varphi i = \gamma$ şi $\varphi j = \delta$. Demonstraţi!

În cazul algebrelor polinomiale clasice se obţine următoarea teoremă importantă, care formalizează şi dă un sens precis expresiei „*se dau valorile* $a_1, \ldots, a_n$ *nedeterminatelor* $X_1, \ldots, X_n$” :

1.13 Teoremă. *Fie R un inel comutativ şi A o R-algebră.*

a) (Proprietatea de universalitate a algebrei de polinoame $R[X]$) *Pentru orice $a \in A$ există un unic morfism de R-algebre $v_a : R[X] \to A$ cu proprietatea că $v_a(X) = a$.*

b) (Proprietatea de universalitate a algebrei de polinoame $R[X_1,\ldots, X_n]$) *Fie $n \in \mathbb{N}^*$ fixat. Pentru orice n-uplu $\mathbf{a} = (a_1,\ldots,a_n) \in A^n$ există un unic morfism de R-algebre $v_\mathbf{a} : R[X_1,\ldots, X_n] \to A$ astfel încît $v_\mathbf{a}(X_i) = a_i$, $\forall i \in \{1,\ldots, n\}$.*

c) (Proprietatea de universalitate a inelului de polinoame $R[X; S]$) *Fie S o mulţime nevidă. Pentru orice aplicaţie $\gamma : S \to A$ există un unic morfism de R-algebre $v_\gamma : R[X; S] \to A$ astfel încît $v_\gamma(X_s) = \gamma(s)$, $\forall s \in S$.*

Demonstraţie. Propunem cititorului să demonstreze direct *a)* şi *b)*. Punctul *a)* este un caz particular al lui *b)*, care se obţine la rîndul său din *c)* punînd $S = \{1, \ldots, n\}$. Pentru a demonstra *c)*, observăm că γ induce un morfism de monoizi

$$\beta : \mathbb{N}^{(S)} \to (A, \cdot),\ \beta(\mathbf{i}) = \prod_{s\in \operatorname{supp}(\mathbf{i})} \gamma(s)^{\mathbf{i}(s)},\ \forall \mathbf{i} \in \mathbb{N}^{(S)}$$

Aplicînd proprietatea de universalitate a algebrei monoidale $R[\mathbb{N}^{(S)}] = R[X;\ S]$, rezultă existenţa unui morfism de R-algebre $v_\gamma : R[X;\ S] \to A$ astfel încît $v_\gamma \circ j = \beta$, unde $j : \mathbb{N}^{(S)} \to R[X; S]$ este aplicaţia canonică; în cazul nostru $j(\mathbf{e}_s) = X_s$, $\forall s \in S$. Deci $v_\gamma(X_s) = \beta(\mathbf{e}_s) = \gamma(s)$.

Unicitatea lui v_α rezultă astfel: dacă $v : R[\mathbb{N}^{(S)}] \to A$ este un morfism de R-algebre cu $v(X_s) = \gamma(s)$, atunci $v\circ j = \beta$, unde β este morfismul definit mai sus. Din partea de unicitate a proprietăţii de universalitate a algebrei monoidale rezultă că $v = v_\alpha$. □

Morfismul v_a (respectiv $v_{\mathbf{a}}$) care apare la punctele *a)* şi *b)* se numeşte *morfismul de evaluare*; dacă $\mathbf{a} = (a_1, \ldots, a_n) \in A^n$ şi $f \in R[X_1, \ldots, X_n]$, atunci $v_{\mathbf{a}}(f)$ se notează prin tradiţie $f(a_1, \ldots, a_n)$ şi se numeşte *valoarea polinomului f în* $(a_1, \ldots, a_n)$. Aşadar:

$\forall f = \sum_{i=0}^{n} b_i X^i \in R[X]$, $\forall a \in A$, avem $v_a(f) = f(a) = \sum_{i=0}^{n} b_i a^i$;

$\forall f = \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} b_{i_1\ldots i_n} X_1^{i_1} \ldots X_n^{i_n} \in R[X_1,\ldots, X_n]$, $\forall \mathbf{a} = (a_1, \ldots, a_n) \in A^n$, avem

$$v_{\mathbf{a}}(f) = f(a_1,\ldots,a_n) = \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} b_{i_1\ldots i_n} a_1^{i_1} \ldots a_n^{i_n}.$$

Este important de observat că procedura de „a da valori nedeterminatei”, formalizată în teorema de mai sus, determină algebra polinomială pînă la un izomorfism (cf. Obs. 1.12). Cum formulaţi această proprietate pentru $R[X]$, respectiv $R[X_1,\ldots, X_n]$?

O proprietate utilă a R-algebrelor $R[X_1,\ldots, X_n]$ (uneori folosită pentru a le *defini* recursiv după n) este:

1.14 Teoremă. *Fie* $n \geq 1$. *Atunci există un izomorfism canonic de R-algebre:*

$$R[X_1,\ldots, X_n] \cong R[X_1,\ldots, X_{n-1}][X_n].$$

Demonstraţie. Folosim 1.13.*b)*: $\exists!\ \varphi : R[X_1,\ldots, X_n] \to R[X_1,\ldots, X_{n-1}][X_n]$, φ morfism de R-algebre, cu $\varphi(X_i) = X_i$, $1 \leq i \leq n$. Fie $A := R[X_1,\ldots, X_{n-1}]$.

Invers, din 1.13.*b)* aplicat lui $R[X_1,\ldots, X_{n-1}]$, $\exists!\ \alpha : R[X_1,\ldots, X_{n-1}] \to R[X_1,\ldots, X_n]$, α morfism de R-algebre, cu $\alpha(X_i) = X_i$, $1 \leq i \leq n-1$. Astfel, $R[X_1,\ldots, X_n]$ devine o A-algebră de morfism structural α. Proprietatea de universalitate a A-algebrei de polinoame $A[X_n]$ arată că există un unic $\beta : A[X_n] \to R[X_1,\ldots, X_n]$, β morfism de A-algebre şi $\beta(X_n) = X_n$. Evident, β este şi morfism de R-algebre.

Arătăm că $\beta\varphi = \mathrm{id}$. $\beta\varphi : R[X_1,\ldots, X_n] \to R[X_1,\ldots, X_n]$ este morfism de R-algebre cu $\beta\varphi(X_i) = X_i$, $1 \leq i \leq n$, iar $\mathrm{id} : R[X_1,\ldots, X_n] \to R[X_1,\ldots, X_n]$ are aceleaşi proprietăţi. Partea de unicitate de la 1.13.*b)* arată că $\beta\varphi = \mathrm{id}$. La fel, $\varphi\beta = \mathrm{id}$, deci φ este izomorfism. □

În continuare, facem cîteva consideraţii asupra noţiunii de *grad* al unui polinom.

Dacă aX^n este un monom în $R[X]$ (cu $a \neq 0$), n se numeşte *gradul* lui aX^n. Punem grad $0 = -\infty$.

Dacă $g \in R[X]$, $g = a_0 + a_1X + \ldots + a_nX^n$, cu $a_n \neq 0$, numărul natural n se numeşte *gradul* lui g, notat grad g (sau deg g) [50]. Deci gradul lui g este cel mai mare grad al monoamelor lui g. Elementele $a_0, \ldots, a_n \in R$ se numesc *coeficienţii* polinomului g, iar a_n se numeşte *coeficientul dominant* al lui g.

Dacă $aX_1^{i_1} \ldots X_n^{i_n}$ este un monom în $R[X_1,\ldots, X_n]$ (cu $a \neq 0$), şi $1 \leq k \leq n$, definim *gradul în* X_k: $\text{grad}\left(aX_1^{i_1} \ldots X_n^{i_n}, X_k\right) := i_k$ (exponentul lui X_k în monom). Pentru un polinom $g \in R[X_1,\ldots, X_n]$, grad (g, X_k) este cel mai mare grad în X_k al monoamelor lui g. Dacă R este inel integru, atunci gradul este *aditiv*: $\forall g, h \in R[X_1,\ldots, X_n]$,

$$\text{grad}\,(gh, X_k) = \text{grad}\,(g, X_k) + \text{grad}\,(h, X_k).$$

Avem şi:

$$\text{grad}\,(g + h, X_k) \leq \max(\text{grad}\,(g, X_k), \text{grad}\,(h, X_k)).$$

Este utilă şi noţiunea de *grad total*: gradul total al monomului $aX_1^{i_1} \ldots X_n^{i_n}$ este $i_1 + \ldots + i_n$; gradul total al unui polinom g este cel mai mare grad total al monoamelor sale. În general, cînd se vorbeşte fără alte precizări de „gradul” unui polinom în mai multe nedeterminate, este vorba de gradul său total. Un polinom care are toate monoamele de acelaşi grad se numeşte *polinom omogen* sau *formă*. Şi gradul total este aditiv, dacă R este integru.

III.2 Corpul numerelor complexe construit ca inel factor

Unul din motoarele dezvoltării matematicii, a algebrei în special, a fost, pînă la mijlocul secolului XIX, *rezolvarea ecuaţiilor polinomiale* cu coeficienţi reali (remarcăm totuşi că o teorie riguroasă a corpului numerelor reale apare abia în a doua jumătate a sec. XIX). Însă ecuaţii polinomiale foarte simple, de exemplu $X^2 + 1 = 0$, *nu au soluţii reale*: formal, „soluţia” acestei ecuaţii este „rădăcina pătrată din – 1” care, evident, *nu* este un număr real. Încă din sec. XVI s-au folosit „cantităţi” de tipul $i = \sqrt{-1}$ în exprimarea soluţiilor ecuaţiilor şi s-a observat că se poate opera în mod coerent cu „numere” de forma $a + bi$, cu a şi b numere reale: ele se adună şi se înmulţesc conform regulilor „uzuale” (adică se respectă proprietăţile de comutativitate, distributivitate, …, care se regăsesc în axiomele corpului), cu menţiunea (oarecum şocantă) că $i^2 = -1$. Numerele de forma bi au fost numite *numere pur imaginare*, pentru a sublinia că *nu* este vorba de numere reale. Cum se poate face însă pe baze riguroase construcţia „numerelor complexe”?

---

[50] De la englezescul *degree* (sau francezul *degré*).

În general, construcția care se dă corpului $\mathbb{C}$ al numerelor complexe este următoarea: se definește $\mathbb{C} = \mathbb{R}\times\mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}$ și se înzestrează $\mathbb{C}$ cu două operații, adunarea și înmulțirea, astfel:

$(a, b) + (c, d) := (a + c, b + d)$; $(a, b)\cdot(c, d) := (ac - bd, ad + bc)$, $\forall(a, b), (c, d) \in \mathbb{C}$

Dacă definiția adunării este naturală și este clar că $(\mathbb{C}, +)$ este grup abelian, nu este clar de ce se definește astfel *înmulțirea*; în plus, nu este deloc evident că avem de a face cu o operație asociativă, distributivă față de adunare, care are element neutru și că orice element nenul (diferit de $(0, 0)$) are invers. Aceste fapte sînt consecința unor verificări directe care aduc prea puțină lumină în *motivarea* definiției înmulțirii.

Există o abordare naturală a construcției lui $\mathbb{C}$, folosind noțiuni elementare de algebră: *inele factor, teorema de izomorfism* și *teorema împărțirii cu rest în inele de polinoame*.

Începem cu această ultimă teoremă, de o importanță ce nu poate fi îndeajuns subliniată.

2.1 Teoremă (teorema împărțirii cu rest în inele de polinoame) *Fie K un corp comutativ și $f, g \in K[X]$, cu $g \neq 0$. Atunci există două polinoame $q, r \in K[X]$ astfel încît $f = gq + r$, unde $r = 0$ sau* grad $r <$ grad g.

În plus, q, r sînt unic determinate cu proprietățile de mai sus.

Demonstrație. Demonstrația este inspirată din algoritmul de împărțire a polinoamelor predat în școală. Fie $f = a_0 + \ldots + a_nX^n$ și $g = b_0 + \ldots + b_mX^m$ polinoame din $K[X]$, cu $g \neq 0$ (adică $b_m \neq 0$). Facem o inducție după $n =$ grad f. Dacă $n < m$, punem $q = 0$, $r = f$. Dacă $n \geq m$, polinomul $h := f - b_m^{-1}a_nX^{n-m}g$ are gradul strict mai mic decît n (termenii de grad n se reduc, de aceea am și ales coeficienții astfel) și, din ipoteza de inducție, putem scrie $h = gq + r$, cu grad $r < m$. Astfel, $f = g\left(q + b_m^{-1}a_nX^{n-m}\right) + r$. Unicitatea e propusă ca exercițiu. □

Problema construcției lui $\mathbb{C}$ poate fi reformulată în termeni mai preciși astfel:

Considerăm în $\mathbb{R}[X]$ polinomul $f = X^2 + 1$, care este ireductibil în $\mathbb{R}[X]$ (căci nu are rădăcini în $\mathbb{R}$ și este de grad 2). Căutăm o *extindere a lui* $\mathbb{R}$ (adică un corp $\mathbb{C}$, în care $\mathbb{R}$ să fie subcorp) în care polinomul f să aibă o rădăcină. Acesta este un caz particular al unei probleme fundamentale în teoria ecuațiilor polinomiale:

2.1 Problemă. *Fie K un corp și $f \in K[X]$ un polinom ireductibil, grad $f \geq 2$ (deci f nu are rădăcini în K). Există un corp L, extindere a lui K, în care f să aibă o rădăcină? Se poate construi efectiv?*

Presupunem problema rezolvată. Fie L un corp care include K, astfel încît f are o rădăcină α în L. Afirmația „polinomul $f \in K[X]$ are rădăcina α în L" se interpretează riguros astfel: morfismul de evaluare în α, $v_\alpha : K[X] \to L$, $f \mapsto f(\alpha)$, are proprietatea că $v_\alpha(f) = 0$. (L fiind o K-algebră, v_α este bine definit, vezi **III.1.13**)

Considerăm morfismul de evaluare în α,

$$v_\alpha : K[X] \to L,\ v_\alpha(g) = g(\alpha),\ \forall g \in K[X].$$

Atunci $v_\alpha(f) = 0$. În consecință, Ker v_α ($= \{g \in K[X] \mid v_\alpha(g) = 0\}$) este nenul, căci $f \in$ Ker v_α. Teorema fundamentală de izomorfism spune că

$$\begin{aligned} K[X]/\mathrm{Ker}\ v_\alpha &\cong \mathrm{Im} v_\alpha \\ g + \mathrm{Ker}\ v_\alpha &\mapsto v_\alpha(g) \end{aligned} \tag{1}$$

Imv_α este un subinel al lui L, care conține α (de ce?), deci Imv_α (sau mai degrabă $K[X]$/Ker v_α, cu care e izomorf!) ar fi un bun candidat la soluția problemei (dacă ar fi corp!). Să vedem cine e Ker v_α. Cum f este ireductibil, idealul generat de f, notat (f), este *maximal*. Cum $(f) \subseteq$ Ker v_α şi (f) este maximal, $(f) =$ Ker v_α (Ker $v_\alpha \neq K[X]$, căci polinomul constant $1 \notin$ Ker v_α)).[51] Astfel, $K[X]$/Ker $v_\alpha = K[X]/(f)$ este chiar corp, conform teoremei **II.4.8**.

Am găsit soluția problemei: punem $L = K[X]/(f)$. *Putem însă să considerăm corpul K drept un subcorp al lui* $K[X]/(f)$? Există aplicația canonică $\varphi : K \to K[X]/(f)$, $\varphi(a) = \hat{a}$ (clasa lui a modulo (f), notată şi $a + (f)$), $\forall a \in K$, care este morfism de corpuri (de ce?). Cum φ este injectivă[52], se poate identifica $a \in K$ cu imaginea sa $\varphi(a) \in L$, deci K este izomorf cu subcorpul $\varphi(K)$ al lui L. Această situație apare des în teoria corpurilor:

2.2 Definiție. Fie K un corp. Dacă $\sigma : K \to L$ este un morfism de corpuri, atunci tripletul (K, L, σ) se numeşte o *extindere a lui K*. În acest caz, pentru orice element $a \in K$, obişnuim să identificăm $\sigma(a) \in L$ cu $a \in K$. Astfel, dacă $a \in K$ şi $x \in L$, vom scrie $a \cdot x$ în loc de $\sigma(a) \cdot x$ etc. Prin această identificare, K este *subcorp* al lui L şi scriem, prin abuz, „extinderea $K \subseteq L$" în loc de „extinderea (K, L, σ)". Observăm că L este o extindere a lui K dacă şi numai dacă L este un corp care are o structură de K-algebră.

Putem acum formula soluția la problema **2.1** de mai sus:

2.3 Teoremă. *Fie K un corp şi $f \in K[X]$ un polinom ireductibil. Atunci există un corp L, extindere a lui K, în care f are o rădăcină. Mai precis, inelul factor $L := K[X]/(f)$ este corp şi K-algebră prin intermediul aplicației naturale $a \mapsto a + (f) = \hat{a}$ (clasa lui a modulo idealul (f)), iar elementul $\alpha = X + (f) = \hat{X}$ este rădăcină a lui f în L.*

Demonstrație. Faptul că $L = K[X]/(f)$ este corp a fost justificat mai sus; dăm şi o demonstrație „elementară", care furnizează şi un mijloc efectiv de a găsi inverse în $K[X]/(f)$. Fie $\hat{g} \neq \hat{0}$ un element nenul din L, unde $g \in K[X]$. Cum $g \notin (f)$, rezultă $f \nmid g$; ireductibilitatea lui f arată că $(f, g) = 1$. Deci există $u, v \in K[X]$ astfel încît $1 = uf + vg$[53]. Trecînd la clase modulo f, obținem $\hat{1} = \widehat{uf + vg} = \widehat{vg}$. Deci $\hat{g}$ are invers, anume $\hat{v} \in L$.

---

[51] Cititorul "pierdut" de aceasta demonstrație poate găsi una elementară citind toată pagina.
[52] Orice morfism de corpuri este injectiv!
[53] Polinoamele *u* şi *v* se pot găsi efectiv cu *algoritmul extins al lui Euclid*.

Rădăcina lui f în L este $\widehat{X}$ (lucru care poate fi intuit dacă privim la izomorfismul (1) şi căutăm contraimaginea lui α). Într-adevăr, fie $f = a_0 + a_1X + \ldots + a_nX^n$; atunci:
$f(\widehat{X}) = a_0\widehat{1} + a_1\widehat{X} + \ldots + a_n\widehat{X}^n = \widehat{a_0 + a_1X + \ldots + a_nX^n} = \widehat{f} = \widehat{0}$. □

Construcţia lui $\mathbb{C}$. Revenind la $K = \mathbb{R}$ şi $f = X^2 + 1$, rezultă că $\mathbb{R}[X]/(X^2 + 1)$ este un corp în care $i := \widehat{X}$ (clasa lui X modulo idealul $(X^2 + 1)$) este rădăcină a polinomului $X^2 + 1$:

$$i^2 + \widehat{1} = \widehat{X}^2 + \widehat{1} = \widehat{X^2 + 1} = \widehat{0}$$

Să arătăm că putem scrie elementele din $\mathbb{R}[X]/(X^2 + 1)$ sub forma familiară $a + bi$, cu $a, b \in \mathbb{R}$. Un element oarecare din $\mathbb{R}[X]/(X^2 + 1)$ este de forma $\widehat{g} = g + (X^2 + 1)$, cu $g \in \mathbb{R}[X]$. Aplicînd teorema împărţirii cu rest polinoamelor g şi $X^2 + 1$, există $q, r \in \mathbb{R}[X]$ astfel încît:

$$g = (X^2 + 1)q + r,\ \text{ cu grad } r < 2.$$

Deci $r = a + bX$, cu $a, b \in \mathbb{R}$. Trecem la clase modulo $(X^2 + 1)$ în egalitatea de mai sus:

$$\widehat{g} = \widehat{(X^2 + 1)q + r} = \widehat{r} = \widehat{a + bX} = \widehat{a} + \widehat{b}\widehat{X}$$

Dacă ţinem cont că identificăm elementele a din $\mathbb{R}$ cu imaginile lor $\widehat{a} = a + (X^2 + 1))$ din $\mathbb{R}[X]/(X^2 + 1)$, iar $\widehat{X} = i$, egalitatea de mai sus se scrie

$$\widehat{g} = a + bi$$

Scrierea aceasta este unică: dacă $a + bi = c + di$, cu $a, b, c, d \in \mathbb{R}$, atunci $(X^2 + 1)$ divide $a + bX - (c + dX)$ şi rezultă imediat că $a = b$ şi $c = d$.

Ceea ce am făcut nu este altceva decît determinarea unui *sistem de reprezentanţi* pentru clasele din $\mathbb{R}[X]/(X^2 + 1)$; acesta este $\{\widehat{a + bX} \mid a, b \in \mathbb{R}\} = \{a + bi \mid a, b \in \mathbb{R}\}$, clasele tuturor resturilor posibile la împărţirea cu $X^2 + 1$.

Să verificăm şi regula uzuală de înmulţire a două elemente scrise sub forma $a + bi$. Pentru aceasta, ţinînd cont de distributivitate şi că $i^2 = -1$, avem

$$(a + bi)\cdot(c + di) = ac + bdi^2 + adi + bci = ac - bd + (ad + bc)i.$$

Avantajele introducerii lui $\mathbb{C}$ ca $\mathbb{R}[X]/(X^2 + 1)$ sînt următoarele:

- se foloseşte o construcţie (inelul claselor de resturi modulo $(X^2 + 1)$) care are aceeaşi idee de bază ca şi construcţia inelului de clase de resturi modulo n, $\mathbb{Z}_n$;
- construcţia este naturală, are legătură directă cu polinomul $X^2 + 1$ şi ilustrează importanţa teoremei împărţirii cu rest în $\mathbb{R}[X]$ şi a noţiunii de ireductibilitate;
- nu mai este necesar calculul de verificare a îndeplinirii axiomelor corpului (asociativitate, existenţa elementului neutru la adunare şi înmulţire etc.);
- posibilitatea generalizării imediate la construcţii de extinderi de corpuri oarecare, pornind de la polinoame ireductibile.

Vom trece în revistă cîteva dezvoltări ale acestor idei la extinderi oarecare de corpuri. Teorema **2.3** are drept consecinţă:

2.4 Teoremă. *Fie K un corp şi* $f \in K[X]$, $\operatorname{grad} f \geq 1$. *Atunci există o extindere L a lui K, astfel încît f se descompune în factori de gradul* 1 *în* $L[X]$ (*f „are toate rădăcinile în L”*).

Demonstraţie. Inducţie după grad *f*. Mai precis, considerăm afirmaţia $P(n)$: „pentru orice corp *K* şi pentru orice polinom $f \in K[X]$, $\operatorname{grad} f = n$, există o extindere *L* a lui *K* astfel încît *f* se descompune în factori de grad 1 în $L[X]$”. Dacă $n = 1$, atunci extinderea căutată este chiar *K*. Presupunem afirmaţia adevărată pentru orice $t < n$ şi o demonstrăm pentru *n*. Fie deci $f \in K[X]$, $\operatorname{grad} f = n$ şi $g \in K[X]$ un factor ireductibil al lui *f* (*f* se scrie ca un produs de polinoame ireductibile, vezi IV.2.5). Teorema 2.3 asigură că există o extindere *E* a lui *K* în care *g* are o rădăcină α. În $E[X]$, $f = (X - \alpha)h$, cu $h \in E[X]$. Cum $\operatorname{grad} h = n - 1$, îi putem aplica ipoteza de inducţie şi deci există o extindere *L* a lui *E* în care *h* (deci şi *f*) se descompune în produs de factori de grad 1. □

2.5 Definiţie. Fie $K \subseteq L$ o extindere de corpuri. Atunci *L* are o structură canonică de *K*-spaţiu vectorial[54]: înmulţirea unui „scalar” din *K* cu un „vector” din *L* este înmulţirea din *L*. Dimensiunea lui *L* văzut ca spaţiu vectorial peste *K* se numeşte *gradul extinderii* $K \subseteq L$ şi se notează $[L : K]$.

2.6 Definiţie. Fie $K \subseteq L$ o extindere şi $x \in L$. Spunem că *x* este *algebric peste K* dacă există un polinom nenul $f \in K[X]$ astfel încît $f(x) = 0$. Spunem că *x* este *transcendent peste K* dacă nu este algebric peste *K*.

În extinderea $\mathbb{R} \subseteq \mathbb{C}$, elementul $i \in \mathbb{C}$ este algebric peste $\mathbb{R}$, deoarece este rădăcina polinomului $X^2 + 1 \in \mathbb{R}[X]$. Gradul extinderii este $[\mathbb{C} : \mathbb{R}] = 2$, deoarece $\{1, i\}$ este o bază a $\mathbb{R}$-spaţiului liniar $\mathbb{C}$.

Dacă $K \subseteq L$ este o extindere şi $x \in L$ este algebric peste *K*, atunci există un polinom nenul *de grad minim* în $K[X]$ care are rădăcina *x*. Acest polinom este unic determinat dacă cerem să fie unitar (cu coeficientul dominant egal cu 1) şi se numeşte *polinomul minimal al lui x peste K* , notat $\operatorname{Irr}(x, K)$. Are loc următoarea caracterizare a polinomului minimal:

2.7 Teoremă. *Fie* $K \subseteq L$ *o extindere de corpuri şi* $x \in L$, *algebric peste K şi* $v_x : K[X] \to L$, $v_x(g) = g(x)$, $\forall g \in K[X]$ (*morfismul de evaluare în x*). *Fie f un polinom unitar cu coeficienţi în K. Următoarele afirmaţii sînt echivalente:*

a) $f(x) = 0$ *şi* $\operatorname{grad} f = \min\{\operatorname{grad} g \mid g \in K[X], g(x) = 0, g \neq 0\}$.

b) $f(x) = 0$ *şi f este ireductibil.*

c) f este un generator al idealului $\operatorname{Ker} v_x = \{g \in K[X] \mid g(x) = 0\}$.

d) $f(x) = 0$ *şi, oricare ar fi* $g \in K[X]$ *cu* $g(x) = 0$, *rezultă că* $f \mid g$. □

[54] Această interpretare este fundamentală în toată teoria extinderilor de corpuri.

2.8 Exemple. a) $\mathrm{Irr}(\sqrt{2}, \mathbb{Q}) = X^2 - 2$ căci $X^2 - 2 \in \mathbb{Q}[X]$, este unitar, se anulează în $\sqrt{2}$ şi este ireductibil în $\mathbb{Q}[X]$.

b) $\mathrm{Irr}(\sqrt{2}, \mathbb{R}) = X - \sqrt{2}$. În general, pentru orice corp K şi $a \in K$, $\mathrm{Irr}(a, K) = X - a$.

Fie extinderea $K \subseteq L$ şi $x \in L$. Sînt de primă importanţă următoarele noţiuni:

- *subinelul* lui L generat[55] de K şi $\{x\}$, notat $K[x]$. Are loc (demonstraţi):

$$K[x] = \{a_0 + a_1 x + \ldots + a_n x^n \mid n \in \mathbb{N}, a_i \in K, 0 \le i \le n\} = \mathrm{Im}\, v_x. \qquad \text{(S)}$$

- *subcorpul* lui L generat de K şi $\{x\}$, notat $K(x)$. Are loc:

$$K(x) = \{\alpha\beta^{-1} \mid \alpha, \beta \in K[x], \beta \neq 0\}.$$

De exemplu, subcorpul lui $\mathbb{C}$ generat de $\mathbb{Q}$ şi $\sqrt{2}$ este $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ (demonstraţi!). Se observă că nu este nevoie să luăm *toate* expresiile polinomiale (de orice grad) în $\sqrt{2}$, cu coeficienţi în $\mathbb{Q}$, ca în caracterizarea (S), ci doar cele de grad mai mic decît $2 = \mathrm{grad}\,\mathrm{Irr}(\sqrt{2}, \mathbb{Q})$. De asemenea, are loc şi $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$. Lucrul acesta nu este întîmplător şi este caracteristic elementelor *algebrice*:

2.9 Teoremă (de caracterizare a elementelor algebrice). *Fie $K \subseteq L$ o extindere de corpuri şi $x \in L$. Următoarele afirmaţii sînt echivalente:*

a) x este algebric peste K.

b) $K[x]$ este corp.

c) $K[x] = K(x)$.

d) Extinderea $K \subseteq K(x)$ este finită.

Dacă x este algebric peste K şi $f = \mathrm{Irr}(x, K)$, $\mathrm{grad}\, f = n$, atunci $K[X]/(f) \cong K(x)$. În particular, $[K(x) : K] = n$ şi o bază a K-spaţiului liniar $K(x)$ este $\{1, x, \ldots, x^{n-1}\}$.

Demonstraţie. *a)⇒b)* Fie $f = \mathrm{Irr}(x,K) \in K[X]$ şi $v_x : K[X] \to L$ morfismul de evaluare în x. Avem $\mathrm{Ker}\, v_x = f$. Din teorema de izomorfism pentru inele, $K[X]/(f) \cong \mathrm{Im}\, v_x = K[x]$. Cum f este ireductibil în $K[X]$, idealul (f) este maximal şi $K[X]/(f)$ este corp. Atunci $K[x]$, izomorf cu $K[X]/(f)$, este şi el corp.

b)⇔c) Evident.

c)⇒a) Presupunem că $x \neq 0$ şi fie $x^{-1} = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$ inversul lui x. Înmulţind cu x, obţinem $a_0 x + a_1 x^2 + \ldots + a_n x^{n+1} - 1 = 0$, adică x este rădăcina unui polinom nenul cu coeficienţi în K.

d)⇒a) Familia infinită $\{x^i \mid i \in \mathbb{N}\}$ de elemente ale K-spaţiului vectorial finit dimensional $K(x)$ este liniar dependentă. Deci, există o relaţie de dependenţă liniară de forma $a_0 \cdot 1 + a_1 x + \ldots + a_n x^n = 0$, cu $n \in \mathbb{N}$ şi $a_0, a_1, \ldots, a_n \in K$, nu toţi nuli, adică x este algebric peste K.

a)⇒d) Avem K-izomorfismul de corpuri $K[X]/(f) \cong K(x)$. Acesta este şi un izomorfism de K-spaţii vectoriale. Fie $n = \mathrm{grad}\, f$. Demonstrăm că în K-spaţiul vectorial $K[X]/(f)$, clasele

[55] Subinelul lui L generat de o submulţime S a lui L este definit ca intersecţia tuturor subinelelor lui L care includ S. La fel se defineşte subcorpul generat de S.

elementelor $\hat{1}$, $\hat{X}$, ..., $\widehat{X^{n-1}}$ sînt elementele unei baze. Dacă $a_0\hat{1} + a_1\hat{X} + \ldots + a_{n-1}\widehat{X^{n-1}} = \hat{0}$, cu $a_0, a_1, \ldots, a_{n-1} \in K$, atunci $g = a_0 + a_1X + \ldots + a_{n-1}X^{n-1} \in (f)$, adică $f\,|\,g$. Cum grad $f = n$, rezultă că $g = 0$, adică $a_0, a_1, \ldots, a_{n-1}$ sînt nule. Pe de altă parte, folosind teorema împărţirii cu rest, orice clasă modulo f a unui polinom $h \in K[X]$ are un reprezentant de grad mai mic decît n. Aceasta înseamnă că $\hat{h}$ este combinaţie liniară cu coeficienţi în K de $\hat{1}$, $\hat{X}$, ..., $\widehat{X^{n-1}}$.

Izomorfismul $K[X]/(f) \cong K(x)$ duce $X + (f)$ în x, deci baza $\{1, X, ..., X^{n-1}\}$ este dusă în baza $\{1, x, ..., x^{n-1}\}$ în $K[x]$. □

2.10 Definiţie. Fie K un corp şi x un element algebric peste K. Gradul extinderii $K \subseteq K[x]$ (egal cu grad Irr(x, K)) se numeşte *gradul elementului x peste K*.

Fie K un corp. Teorema III.2.4 arată că, *pentru* $f \in K[X]$ *dat*, există o extindere $K \subseteq L$ în care f are toate rădăcinile. Ar fi de dorit să putem găsi un corp Ω, extindere a lui K, încît *orice polinom* $f \in K[X]$ de grad ≥ 1 are toate rădăcinile în Ω. În acest sens, este esenţial conceptul următor:

2.11 Definiţie. Un corp Ω se numeşte corp *algebric închis* dacă orice polinom de grad ≥ 1 din $\Omega[X]$ are cel puţin o rădăcină în Ω.

2.12 Teoremă (*Caracterizarea corpurilor algebric închise*). *Fie* Ω *un corp. Următoarele afirmaţii sînt echivalente:*

a) Ω *este corp algebric închis.*

b) Orice polinom cu coeficienţi în Ω*, de grad* $n \geq 1$ *se descompune în factori liniari în* $\Omega[X]$ (*are n rădăcini în* Ω).

c) Nu există extinderi finite proprii ale lui Ω.

d) Singurele polinoame ireductibile din $\Omega[X]$ *sînt cele de grad* 1.

Demonstraţie. *a)⇒b)* Presupunem prin reducere la absurd că există $f \in \Omega[X]$, grad $f \geq 1$, astfel încît f nu se scrie ca un produs de factori liniari în $\Omega[X]$. Alegem f de grad minim cu această proprietate. Din ipoteză, f are o rădăcină $a \in \Omega$, deci $f = (X - a)g$, cu $g \in \Omega[X]$. Dar grad $g <$ grad f, deci g se descompune în factori liniari. Egalitatea $f = (X - a)g$ arată că şi f se descompune în factori liniari, contradicţie.

b)⇒c) Dacă $\Omega \subseteq L$ este o extindere finită, iar $\alpha \in L \setminus \Omega$, atunci α este algebric peste Ω; fie $g = \mathrm{Irr}(\alpha, \Omega)$. Cum $g \in \Omega[X]$, g are o rădăcină în Ω, deci grad $g = 1$ (g este ireductibil!). Deci $\alpha \in \Omega$, contradicţie.

Restul implicaţiilor sînt lăsate cititorului. □

Are loc următorul rezultat fundamental:

2.13 Teoremă. *Orice corp K are o extindere care este corp algebric închis.* □

Demonstraţia este neconstructivă şi foloseşte Axioma Alegerii (mai precis Lema lui Zorn). Vezi, de exemplu, ION şi RADU [1981] sau TOFAN şi VOLF [2001].

Un exemplu clasic important de corp algebric închis este $\mathbb{C}$. Nu includem o demonstraţie, fiind mai mult tehnică. Aşadar, are loc:

2.14 Teoremă.[56] *Corpul $\mathbb{C}$ al numerelor complexe este algebric închis.* □

III.3 Corpuri finite şi criptografie

Corpurile finite au depăşit de mult stadiul de curiozitate matematică. Corpurile finite sînt esenţiale în tehnologiile legate de transmisia, stocarea, secretizarea şi prelucrarea informaţiei digitale. Codurile liniare corectoare de erori se bazează pe corpuri finite, iar unele din cele mai puternice scheme criptografice moderne au la bază logaritmul discret într-un corp finit.

Clasificarea corpurilor finite este simplă: *pentru orice număr q, putere a unui prim, există un unic (pînă la izomorfism) corp finit cu q elemente, notat* $\mathbb{F}_q$. Acestea sînt toate corpurile finite (pînă la izomorfism). În plus, grupul $(\mathbb{F}_q^*, \cdot)$ este ciclic. Vom demonstra în continuare aceste fapte.

În acest paragraf, „corp” înseamnă „corp comutativ”.

3.1 Teoremă. *Fie F un corp finit cu q elemente. Au loc următoarele afirmaţii:*

a) Există un număr prim p şi $n \in \mathbb{N}^*$ astfel încît $|F| = p^n$.

b) Pentru orice număr prim p şi $n \in \mathbb{N}^*$, există un corp finit cu p^n elemente.

Demonstraţie. a) Fie e elementul unitate al lui F. Atunci mulţimea multiplilor lui e, $P := \{n\cdot e \mid n \in \mathbb{N}^*\}$, este o submulţime a lui F şi este finită. Deci există $p \in \mathbb{N}^*$ astfel încît $p\cdot e = 0$. Alegem p să fie minim cu această proprietate ($p = \operatorname{car} F$, vezi exerciţiul III.3.1). Dacă p nu ar fi prim, atunci $p = ab$, cu $1 < a,\ b < p$. Cum $p\cdot e = (ab)\cdot e = (a\cdot e)\cdot(b\cdot e) = 0$, rezultă că $a\cdot e = 0$ sau $b\cdot e = 0$, contradicţie cu minimalitatea lui p.

Rămîne că există un unic p prim astfel încît $p\cdot e = 0$. Deci $P = \{0, e, 2e, \ldots, (p-1)e\}$. Observăm că există o bijecţie între P şi $\mathbb{Z}_p = \{\hat{0}, \hat{1}, \ldots, \widehat{p-1}\}$ (inelul claselor de

[56] Această teoremă e cunoscută sub numele de *teorema fundamentală a algebrei* sau *teorema d'Alembert-Gauss*. Jean le Rond d'Alembert propune o demonstraţie (incompletă) în 1746. C.F. Gauss dă patru demonstraţii corecte acestei teoreme, prima oară în 1797. Alte demonstraţii au mai fost date de Jean Argand (1814), Augustin Louis Cauchy (1820). Teorema lui Liouville (datorată de fapt lui Cauchy, 1844) –„orice funcţie olomorfă mărginită pe $\mathbb{C}$ este constantă”– demonstrează teorema într-un rînd. Remarcăm că toate demonstraţiile fac apel şi la rezultate de analiză matematică, datorită faptului că proprietăţi fundamentale (topologice) ale corpului $\mathbb{R}$ nu admit descrieri pur algebrice. Rolul esenţial îl joacă mai degrabă proprietăţile de ordine ale lui $\mathbb{R}$.

resturi modulo p), dată de $i \cdot e \mapsto \hat{i}$; . Este chiar un izomorfism, după cum se verifică imediat. Deci P este corp (fiind izomorf cu corpul $\mathbb{Z}_p$), iar F este o extindere a sa.

Interpretăm F ca un spaţiu liniar peste P. Atunci dimensiunea lui F peste P este finită, fie $\dim_P F = n$. Deci $F \cong P^n$ (izomorfism de spaţii liniare), adică $|F| = p^n$.

b) Presupunem problema rezolvată: dacă F este corp finit cu $q := p^n$ elemente, grupul $(F^*, \cdot)$ are $q - 1$ elemente. Aplicînd teorema lui Lagrange, obţinem că $x^{q-1} = 1$, deci $x^q = x$, $\forall x \in F$. Pe de altă parte, din punctul *a)*, F conţine un subcorp izomorf cu $\mathbb{Z}_p$. Deci F este o extindere a lui $\mathbb{Z}_p$, iar $X^q - X \in \mathbb{Z}_p[X]$ se descompune în factori liniari în $F[X]$ (ca în teorema 2.4). Argumentăm acum astfel existenţa unui corp cu $q = p^n$ elemente: fie corpul $\mathbb{Z}_p$ şi $f = X^q - X \in \mathbb{Z}_p[X]$. Din 2.4, există o extindere E a lui $\mathbb{Z}_p$ încît f se descompune în factori liniari în $E[X]$. Considerăm mulţimea $F := \{x \in E \mid x^q = x\}$. Să demonstrăm că F este subcorp al lui E (va fi corpul cu q elemente căutat). Fie $x, y \in F$. Atunci $(xy)^q = x^q y^q = xy$, deci $xy \in F$. Avem şi $(x + y)^q = x^q + y^q$ (vezi lema următoare), deci $x + y \in F$. Dacă $x \neq 0$, atunci $(x^{-1})^q = (x^q)^{-1} = x^{-1}$, deci $x^{-1} \in F$. Elementele lui F sînt exact rădăcinile polinomului f, iar acestea sînt în număr de exact q. Într-adevăr, un polinom de grad q are cel mult q rădăcini (IV.3.13); pe de altă parte, f nu are rădăcini multiple, după cum se vede folosind criteriul cu derivata formală IV.3.16: $f' = qX^{q-1} - 1 = -1$, deci $(f, f') = 1$. □

3.2 Lemă. *Fie F un corp de caracteristică $p > 0$. Atunci aplicaţia $\varphi : F \to F$, $\varphi(x) = x^p$, $\forall x \in F$, este un morfism de corpuri* (numit endomorfismul lui Frobenius[57] *al lui F*). *Dacă F este finit, atunci φ este bijectiv* (*este un* automorfism *al lui F*). *Notînd $q = p^n$, atunci $\varphi^n = \varphi \circ \ldots \circ \varphi$ (de n ori) este morfism, iar $\varphi^n(x) = x^q$, $\forall x \in F$.*

Demonstraţie. Fie $x, y \in F$. Este clar că $\varphi(xy) = \varphi(x)\varphi(y)$. Corpul F fiind comutativ, are loc formula binomului lui Newton:

$$\varphi(x + y) = (x + y)^p = \sum_{0 \le i \le p} C_p^i x^{p-i} y^i = x^p + y^p,$$

ultima egalitate avînd loc pentru că p divide coeficienţii binomiali C_p^i dacă $1 \le i < p$ (de ce?).

Morfismul de corpuri $\varphi : F \to F$ este injectiv, deci bijectiv dacă F este finit.

Avem $(\varphi \circ \varphi)(x) = \varphi(x^p) = (\varphi(x))^p = x^{p^2}$ şi, prin inducţie, $\varphi^n(x) = x^{p^n}$, $\forall x \in F$, $\forall n \in \mathbb{N}$. □

Grupul multiplicativ al unui corp finit este *ciclic*, proprietate care are multe aplicaţii:

3.3 Teoremă. *Fie F un corp finit cu q elemente. Atunci grupul $(F^*, \cdot)$ este ciclic: există $\alpha \in F^*$ astfel încît $F^* = \{\alpha^i \mid 1 \le i \le q - 1\}$. Un astfel de element se numeşte* element primitiv[58] *al lui F.*

---

[57] Ferdinand Georg Frobenius (1849-1917), matematician german.

[58] În cazul extinderilor oarecare, dacă pentru extinderea $K \subseteq L$ există $a \in L$ astfel încît $L = K(a)$, atunci a se numeşte *element primitiv* al extinderii. Un element primitiv al unui *corp finit F* este şi un element primitiv al oricărei extinderi $K \subseteq F$.

Demonstrație. Fie m *exponentul* lui $(F^*, \cdot)$ (vezi exercițiul III.3.2). Tot din exercițiu rezultă că există $\alpha \in F^*$ cu ord $\alpha = m$. Rămîne să arătăm că $m = q - 1$. Dacă $m < q - 1$, atunci polinomul $X^m - 1$ ar avea $q - 1$ rădăcini (toate elementele lui F^*), contradicție. □

3.4 Teoremă. *Orice două corpuri finite care au acelaşi cardinal sînt izomorfe.*

Demonstrație. Fie F, E corpuri finite cu $q = p^n$ elemente (cu p prim) şi $\alpha \in F$ un element primitiv. Atunci $f = X^q - X \in \mathbb{Z}_p[X]$ are rădăcina α în F. Pe de altă parte, f este produs de polinoame ireductibile în $\mathbb{Z}_p[X]$; deci există un (unic) factor ireductibil g al lui f astfel încît $g(\alpha) = 0$. Din III.2.9, grad $g = [\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = [F : \mathbb{Z}_p] = n$. Fie β o rădăcină a lui g în E (g are toate rădăcinile în E), atunci $[\mathbb{Z}_p[\beta] : \mathbb{Z}_p] =$ grad $g = n = [E : \mathbb{Z}_p]$, deci $\mathbb{Z}_p[\beta] = E$. Avem acum izomorfismele (cf. III.2.9): $F = \mathbb{Z}_p[\alpha] \cong \mathbb{Z}_p[X]/(g) \cong \mathbb{Z}_p[\alpha] = E$. □

Corpul finit cu p^n elemente (unic pînă la izomorfism) se notează cu GF(p^n) (Galois Field = corp Galois)[59] sau $\mathbb{F}_{p^n}$.

Din existența unui corp finit F cu p^n elemente rezultă că *există polinoame ireductibile de grad n cu coeficienți în* $\mathbb{Z}_p$: de exemplu, polinomul minimal al unui element primitiv al lui F.

3.5 Propoziție. *Pentru orice* $n \in \mathbb{N}^*$, *există măcar un polinom ireductibil de grad n în* $\mathbb{F}_p[X]$*; pentru orice astfel de polinom f,* $\mathbb{F}_p[X]/(f)$ *este un corp cu* p^n *elemente.* □

Problema construcției efective a unui corp cu p^n elemente se reduce la căutarea unui polinom ireductibil g de grad n în $\mathbb{Z}_p[X]$. Corpul căutat va fi inelul factor $\mathbb{Z}_p[X]/(g)$.

Am determinat corpurile finite în ipoteza că sînt comutative. Este remarcabil faptul că ipoteza aceasta este superfluă: *orice corp finit este comutativ* (Teorema lui Wedderburn[60]). Nu includem o demonstrație.

Aplicație. ***Logaritmul discret într-un corp finit. Criptografie. Semnături digitale***

Fie p un număr prim fixat şi $q = p^t$, cu $t \geq 1$. Fie $F = \mathbb{F}_q$, corpul cu q elemente. Fie b un element primitiv al lui F, adică b generează grupul multiplicativ F^*. Atunci orice $a \in F^*$ poate fi scris în mod unic sub forma

$$a = b^r,$$

unde $r \in \mathbb{N}$ şi $0 \leq r \leq q - 2$. Numărul r se numeşte *logaritmul discret al lui a în baza b* şi se notează $\log_b(a)$ sau $\text{ind}_b a$.

Date b şi a ca mai sus, determinarea algoritmică a lui $\log_b(a)$ este cunoscută ca *problema logaritmului discret* (Discrete Logarithm Problem, DLP). Pe baza unui mare număr de fapte teoretice şi practice, DLP este *presupusă ca fiind dificilă* (pentru q mare, ales judicios), mai

---

[59] Structura corpurilor finite a fost determinată de Galois în 1830.
[60] Joseph Henry MacLagen Wedderburn (1882-1948), matematician scoțian.

precis spus *intratabilă computaţional*, în sensul că un calcul efectiv al lui $\log_b(a)$ ar lua sute de ani cu algoritmii şi mijloacele *cunoscute* de calcul, pentru valori curent folosite ale lui q şi b.

Fie $w = [\log_2 r] + 1$ (numărul de biţi din reprezentarea lui r în baza 2). Algoritmul de ridicare la putere dat de exerciţiul III.3.8 calculează b^r (b şi r fiind date) şi cere cel mult $2w$ înmulţiri, adică are un timp de rulare de ordinul $O(w)$. Astfel, *verificarea* faptului că $r = \log_b(a)$ poate fi făcută foarte rapid.

Algoritmul evident (şi total ineficient) de găsire a lui $\log_b(a)$ prin căutare exhaustivă (se calculează toate puterile lui b pînă se găseşte a) cere în cel mai rău caz $q - 1$ ridicări la putere (sau înmulţiri) şi teste de egalitate, fiind prohibitiv din acest punct de vedere. De exemplu, dacă q are 512 cifre binare (se folosesc astfel de q în scheme criptografice actuale), iar o ridicare la putere în $\mathbb{F}_q$ durează 10^{-12}s, 1000 de calculatoare calculînd în paralel au nevoie cam de $2^{512}\cdot 10^{-15}$ secunde de găsire a lui $\log_b(a)$ prin această metodă, adică aproximativ 10^{140} secunde. Vîrsta Universului este estimată la 14 miliarde de ani, aproximativ $5\cdot 10^{17}$ secunde.

Întrebare. Vi se par plauzibile aceste estimări? De ce? Dar dacă q are 128 de cifre binare?

Criptosistemul ElGamal

Se fixează următorii parametri: q (o putere a unui număr prim) şi un element primitiv g al lui $\mathbb{F}_q$ şi se fac publice către toţi utilizatorii. Utilizatorul A are o *cheie privată* a, $2 \le a \le q - 2$ (a este cunoscută doar de A) şi publică $y = g^a \in \mathbb{F}_q^*$. Dacă un utilizator B vrea să trimită un mesaj secret m (presupunem că $m \in F_q^*$) lui A, atunci B alege la întîmplare k, $2 \le k \le q - 2$ şi calculează în $\mathbb{F}_q^*$

$$y_1 = g^k \text{ şi } y_2 = my^k.$$

Cuplul (y_1, y_2) („mesajul cifrat”) este trimis de B lui A. Deoarece

$$m = (mg^{ak})g^{-ak} = y_2(g^{-k})^a = y_2(y_1^{-1})^a,$$

A poate descifra mesajul m calculînd $m = y_2(y_1^{-1})^a$.

Dacă o persoană neautorizată C interceptează (y_1, y_2) (şi, evident, cunoaşte y, cheia publică a lui A), C nu poate descoperi mesajul m decît calculînd k sau a (ambele implicînd calcularea logaritmului discret în baza g: $k = \log_g y_1$, $a = \log_g y$). Un ipotetic algoritm rapid de găsire a DLP ar permite deci descifrarea rapidă a mesajului secret m. Nu s-a găsit un mijloc de a sparge această metodă de cifrare fără calculul logaritmului discret.

Algoritmul de semnătură digitală ElGamal

Semnarea digitală a unui mesaj m este o modalitate de a asigura un utilizator B că un anumit mesaj m (despre care B crede că provine de la un utilizator A) este într-adevăr trimis de A şi nu de cineva care doreşte să se dea drept A.[61] Pentru aceasta, se anexează mesajului m o „semnătură digitală” (un şir de simboluri[62]). Iată un mod de a face aceasta:

[61] Puteţi da exemplu de o astfel de situaţie în practică?
[62] Semnătura electronică trebuie să depindă de A (evident), dar şi de *m*! De ce?

Algoritmul de semnătură ElGamal

Fie $\{0, 1\}^*$ mulțimea şirurilor de elemente din mulțimea $\{0, 1\}^*$ (şiruri de biți, interpretate ca mulțimea tuturor mesajelor posibile).

A publică un număr prim p, un element primitiv $g \in \mathbb{Z}_p^*$, şi un întreg α, $1 \le \alpha \le p - 2$, care este generat prin alegerea unui întreg aleator a, care este ținut secret, şi calculînd $\alpha = g^a$. Cheia publică a lui A este (p, g, α). Cheia privată este a.

Numărul prim p şi elementul primitiv g pot fi aceleaşi pentru toți utilizatorii, caz în care cheia publică a lui Alice este doar α. Alice are nevoie de o *funcție hash*[63] public cunoscută $h : \{0, 1\}^* \to \{1, 2, \dots, p - 2\}$. O funcție hash transformă un mesaj (lung) $m \in \{0, 1\}^*$ într-un cuvînt de lungime fixată numit *valoarea hash* a mesajului (eng. *hashcode*). Valoarea hash are rolul unui reprezentant scurt al şirului de intrare, şi poate fi folosit ca şi cum are identifica în mod unic acel şir. O funcție hash trebuie sa fie *tare rezistentă la coliziuni* (*strong collision resistant*) dacă este nefezabil să se calculeze două mesaje distincte $x, y \in \{0, 1\}^*$ astfel încît $h(x) = h(y)$ (o *coliziune* a lui h). Există la ora actuală mulți algoritmi de calcul pentru funcții hash (MD5, MD6, SHA-512,)

Pentru semnarea unui mesaj $m \in \{0, 1\}^*$, Alice calculează o pereche de numere întregi (r, s), $1 \le r, s < p - 1$, astfel încît

$$g^{h(m)} = \alpha^r r^s \bmod p$$

Pentru a genera r şi s, Alice alege un întreg aleator k cu $(k, p - 1) = 1$ şi calculează $r = g^k \bmod p$. Cum $\alpha = g^a$, aceasta înseamnă că s trebuie să satisfacă

$$g^{h(m)} = g^{ar + ks} \bmod p,$$

ceea ce e echivalent cu $h(m) = ar + ks \pmod{p - 1}$. Cum $(k, p - 1) = 1$, această ecuație are o unică soluție modulo $p - 1$, $s = k^{-1}(h(m) - ar) \pmod{p - 1}$.

Semnătura mesajului m este perechea (r, s). Alice trimite mesajul m şi semnătura (r, s) lui Bob.

Verificare. Bob verifică dacă (r, s) este semnătura lui Alice a documentului m. Mai întîi, verifică dacă $1 \le r < p - 1$. Dacă aceasta nu este adevărat, semnătura e respinsă; altminteri semnătura e acceptată dacă şi numai dacă:

$$g^{h(m)} = \alpha^r r^s \bmod p$$

Un algoritm eficient de calcul al logaritmului discret ar face această schemă nesigură, căci ar da posibilitatea falsificatorului să calculeze a din α şi să genereze semnături care trec testul de verificare a semnăturilor lui Alice, pentru orice m doreşte (falsificare universală). Nu s-a găsit vreo modalitate de a sparge această schemă fără calculul logaritmului discret.

Institutul Național de Standarde şi Tehnologii al S.U.A. (National Institute of Standards and Technology, NIST) a stabilit *Standardul de Semnătură Digitală* (*Digital Signature*

---

[63] Unul din sensurile cuvântului *hash* (eng.) este "mărunțire urmată de amestecare".

Standard, DSS), care este bazat pe o variantă a algoritmului de semnătură ElGamal de mai sus. DSS este standardul de autentificare digitală al guvernului Statelor Unite.

Exerciții

1. (Caracteristica unui inel) Fie K un inel şi e elementul său unitate. Dacă există $k \in \mathbb{N}^*$ astfel încît $ke = 0$, atunci definim car $K = \min\{k \in \mathbb{N}^* \mid ke = 0\}$. În caz contrar, punem car $K = 0$.

a) Demonstrați că, dacă K este integru, atunci car $K = 0$ sau un număr prim.

b) Dacă K este corp de caracteristică $p > 0$, atunci K are un unic subcorp izomorf cu $\mathbb{Z}_p$.

c) Dacă K este corp de caracteristică 0, atunci K are un unic subcorp izomorf cu $\mathbb{Q}$.

2. Fie $(G, \cdot)$ un grup finit. Definim *exponentul* lui G, $\exp(G) := \text{cmmmc}\{\text{ord } a \mid a \in G\} = \min\{n \mid x^n = 1, \forall x \in G\}$.[64] Să se arate că:

a) Dacă $a, b \in G$, $ab = ba$ şi $(\text{ord } a, \text{ord } b) = 1$, atunci $\text{ord } ab = (\text{ord } a)\cdot(\text{ord } b)$.

b) Pentru orice $a, b \in G$ cu $ab = ba$, există $c \in G$ cu $\text{ord} c = [\text{ord } a, \text{ord } b]$.

c) Dacă G este abelian, există un element al lui G care are ordinul egal cu $\exp(G)$.

3. Dacă R este inel comutativ integru, iar G este un subgrup finit al lui $(U(R), \cdot)$, atunci G este ciclic.

4. Dacă F este un corp cu p^n elemente, iar K este un subcorp al său, atunci există $m|n$ astfel încît $|K| = p^m$. Reciproc, pentru orice divizor m al lui n există un unic subcorp al lui F cu $p^m =: r$ elemente, anume $K = \{x \in F \mid x^r = x\}$.

5. Fie F un corp finit şi $m \in \mathbb{N}^*$. Demonstrați că există un polinom ireductibil de grad m în $F[X]$.

6. Construiți corpuri finite cu 4, 8, 16, 25, 9 şi 27 elemente. Pentru fiecare din ele găsiți cîte un element primitiv.

7. (Numărul polinoamelor ireductibile de grad m cu coeficienți într-un corp finit) Fie $F \subseteq L$ o extindere de grad m de corpuri finite, unde F are q elemente. Pentru orice $d \in \mathbb{N}^*$, notăm $P_{q,d} = \{f \in F[X] \mid \text{grad} f = d, f \text{ ireductibil şi unitar}\}$.

a) Demonstrați că $X^{q^m} - X = \prod_{\alpha \in L}(X - \alpha) = \prod_{d|m}\prod_{f \in P_{q,d}} f$.

b) Notăm cu $R_f = \{\alpha \in L \mid f(\alpha) = 0\}$, $\forall f \in F[X]$. Arătați că $\bigcup\{R_f \mid f \in P_{q,d},\ d|m\} = L$ (reuniune disjunctă).

c) Demonstrați că $q^m = \sum_{d|m} |P_{q,d}|\cdot d$.

d) Calculați $P_{2,m}$ şi $P_{3,m}$, $1 \le m \le 6$.

[64] Din teorema lui Lagrange, $\exp(G)$ divide cardinalul lui G.

8. Scrieți un algoritm eficient de calcul al lui b^r, unde b este un element dintr-un inel sau monoid pentru care se cunoaşte un algoritm de înmulțire a două elemente oarecare, iar r este un număr natural. (Ind. Folosiți ridicări la pătrat repetate şi pe înmulțiri cu b, cînd e cazul. Exemplu: pentru a calcula $a = b^{22}$, scriem mai întîi 22_{10} în baza 2, $22 = 10110_2$ şi calculăm succesiv $a = b$, $b^2 = a*a$, $b^5 = (a*a)*b$, $b^{10} = a*a$, $b^{21} = (a*a)*b$. Vezi tabel:

Pasul	0	1	2	3	4
Cifra binară a lui r	1	0	1	1	0
Valoarea lui a	b	$b^2 = a*a$	$b^5 = (a*a)*b$	$b^{11} = (a*a)*b$	$b^{22} = a*a$

III.4 Polinoame simetrice

Fie R un inel comutativ unitar, fixat. Fie $n \in \mathbb{N}^*$ şi $\sigma \in S_n$ (grupul permutărilor de n obiecte). Există un unic morfism de R-algebre $\varphi_\sigma : R[X_1,\dots, X_n] \to R[X_1,\dots, X_n]$ astfel încît $\varphi_\sigma(X_i) = X_{\sigma(i)}$, $\forall i = 1,\dots, n$ (am folosit **1.13** – proprietatea de universalitate a R-algebrei de polinoame $R[X_1,\dots, X_n]$). Dacă $g \in R[X_1,\dots, X_n]$, atunci

$$\varphi_\sigma(g) = g(X_{\sigma(1)},\dots, X_{\sigma(n)}).$$

4.1 Definiție. Fie R un inel comutativ unitar şi $g \in R[X_1,\dots, X_n]$. Spunem că g este *polinom simetric* în $R[X_1,\dots, X_n]$ dacă, $\forall \sigma \in S_n$, are loc $\varphi_\sigma(g) = g$.

Dacă R este integru, de corp de fracții K, considerăm $K(X_1,\dots, X_n)$ (corpul de fracții al inelului integru $R[X_1,\dots, X_n]$, numit *corpul fracțiilor raționale* în nedeterminatele $X_1,\dots, X_n$ cu coeficienți în K). Se defineşte noțiunea de fracție rațională simetrică, astfel: φ_σ se prelungeşte la un unic morfism de corpuri (notat tot cu φ_σ) $\varphi_\sigma : K(X_1,\dots, X_n) \to K(X_1,\dots, X_n)$; are loc, $\forall g$, $h \in R[X_1,\dots, X_n]$, $h \neq 0$: $\varphi_\sigma(g/h) = \varphi_\sigma(g)/\varphi_\sigma(h)$. Fracția rațională $g/h \in K(X_1,\dots, X_n)$ se numeşte *simetrică* dacă, $\forall \sigma \in S_n$, are loc $\varphi_\sigma(g/h) = g/h$.

4.2 Exemple. În $R[X_1, X_2, X_3]$, polinoamele următoare sînt simetrice: $X_1 + X_2 + X_3$, $X_1 X_2 X_3$, $X_1^2X_2 + X_1^2X_3 + X_2^2X_1 + X_2^2X_3 + X_3^2X_1 + X_3^2X_2$. Polinomul $X_1 + X_2$ nu este simetric în $R[X_1, X_2, X_3]$ (dar este simetric în $R[X_1, X_2]$).

4.3 Observații. a) Mulțimea polinoamelor simetrice este o subalgebră a lui $R[X_1,\dots, X_n]$: dacă g, $h \in S$, atunci $\varphi_\sigma(g + h) = \varphi_\sigma(g) + \varphi_\sigma(h) = g + h$, $\forall \sigma \in S_n$. Analog se verifică celelalte condiții.

Arătați că, dacă K este corp, atunci fracțiile raționale simetrice din $K(X_1,\dots, X_n)$ formează *un subcorp*.

b) Dacă $aX_1^{i_1}\dots X_n^{i_n}$ apare ca monom în polinomul simetric $g \in R[X_1,\dots, X_n]$, atunci, $\forall \sigma \in S_n$, $aX_{\sigma(1)}^{i_1}\dots X_{\sigma(n)}^{i_n}$ apare ca monom în g.

4.4 Definiţie. Fie $n \in \mathbb{N}^*$ şi $0 \le k \le n$. Se numeşte *polinom simetric fundamental* (sau *elementar*) de grad k în $R[X_1,\dots, X_n]$ polinomul

$$s_k := \sum\{\prod_{i\in I} X_i \mid I \subseteq \{1, \dots, n\}, |I| = k\}.$$

s_k este aşadar suma tuturor produselor de k nedeterminate distincte alese din $\{X_1,\dots, X_n\}$; s_k are aşadar C_n^k monoame. Prin convenţie, se pune $s_k = 0$ pentru $k > n$ şi $s_0 = 1$. Polinomul s_k este *omogen* de grad k (toate monoamele sale au gradul k). Întrucît s_k depinde de numărul nedeterminatelor, uneori vom nota $s_k(X_1,\dots, X_n)$ pentru a evita confuziile. De exemplu, pentru $n = 4$:

$$s_0 = 1$$
$$s_1 = X_1 + X_2 + X_3 + X_4$$
$$s_2 = X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4$$
$$s_3 = X_1X_2X_3 + X_1X_2X_4 + X_1X_3X_4 + X_2X_3X_4$$
$$s_4 = X_1X_2X_3X_4$$

Polinoamele simetrice fundamentale apar în relaţiile dintre coeficienţii şi rădăcinile unui polinom.

4.5 Teoremă. *a) Fie $n \in \mathbb{N}^*$ şi $s_k = s_k(X_1, \dots, X_n)$. În $R[X_1,\dots, X_n][X]$ are loc relaţia:*

$$(X - X_1)\dots(X - X_n) = X^n - s_1X^{n-1} + s_2X^{n-2} - \dots + (-1)^n s_n.$$

b) Dacă R este subinel al inelului integru S şi $g = a_0 + a_1X + \dots + a_nX^n \in R[X]$ are rădăcinile $x_1, \dots, x_n \in S$, atunci $a_ns_k(x_1, \dots, x_n) = (-1)^k a_{n-k}$.

Demonstraţie. *a)* Inducţie după n (exerciţiu).

b) Există un unic morfism de R-algebre $\varphi : R[X_1,\dots, X_n][X] \to S[X]$ astfel încît $\varphi(X_i) = x_i$ şi $\varphi(X) = X$. Avem, din *a)*:

$$\varphi(a_n(X - X_1)\dots(X - X_n)) = a_n(X - x_1)\dots(X - x_n) = a_n(X^n - s_1X^{n-1} + s_2X^{n-2} - \dots + (-1)^n s_n).$$

Pe de altă parte, $a_n(X - x_1)\dots(X - x_n) = g$ (în corpul de fracţii K al lui S, au aceleaşi rădăcini şi acelaşi coeficient dominant). Se identifică acum coeficienţii. □

4.6 Lemă. *a) Fie $(A, \le)$ şi $(B, \le)$ două mulţimi bine ordonate. Atunci $A\times B$ este o mulţime bine ordonată de ordinea lexicografică dată de:*

$$(a, b) \le (a', b') \text{ dacă şi numai dacă } a < a' \text{ sau } (a = a' \text{ şi } b \le b').$$

b) Într-o mulţime bine ordonată $(A, \le)$ nu există şiruri infinite strict descrescătoare.

c) $\forall n \in \mathbb{N}$, mulţimea T_n a termilor din $R[X_1,\dots, X_n]$ este bine ordonată de ordinea lexicografică (deci nu există un şir infinit strict descrescător de termi).

Demonstraţie. *a)* Reamintim că mulţimea ordonată $(A, \le)$ se numeşte *bine ordonată* dacă *orice submulţime nevidă a lui A are un prim element*. Fie $S \subseteq A\times B$, nevidă. Cum $S_1 := \{a \in A \mid \exists b \in B \text{ cu } (a, b) \in S\} \ne \emptyset$, iar A este bine ordonată, există primul său element

$\alpha \in S_1$ (deci $\forall(a, b) \in S$, $\alpha \le a$). Fie $S_2 := \{b \in B | (\alpha, b) \in S\}$. Există primul element β al lui S_2. Atunci (α, β) este primul element al lui S: $\forall(a, b) \in S$, avem sau $\alpha < a$ (deci $(\alpha, \beta) < (a, b)$) sau $\alpha = a$, caz în care $b \in S_2$, deci $\beta \le b$.

b) Fie $(a_n)_{n \ge 1}$ un şir descrescător de elemente din A. Atunci mulţimea $\{a_n \mid n \ge 1\}$ are un prim element, fie acesta a_k. Pentru $n \ge k$, avem deci $a_k \le a_n$; cum $a_n \le a_k$ (şirul este descrescător), rezultă $a_n = a_k$ şi şirul nu este strict descrescător.

c) Inducţie după n. Dacă $n = 1$, $T_1 = \{X^n \mid n \in \mathbb{N}\}$ este izomorfă ca mulţime ordonată cu $(\mathbb{N}, \le)$, care este bine ordonată. Dacă $n > 1$, T_n cu ordinea lexicografică este izomorfă cu $T_{n-1} \times T_1$ cu ordinea definită ca la punctul *a)*. Din ipoteza de inducţie, T_{n-1} este bine ordonată şi din *a)* rezultă $T_{n-1} \times T_1$ bine ordonată.

4.7 Teoremă. (Teorema fundamentală a polinoamelor simetrice) *Fie R un inel comutativ unitar şi g un polinom simetric din* $R[X_1,\ldots, X_n]$. *Atunci există un unic polinom* $h \in R[X_1,\ldots, X_n]$ *astfel încît* $g = h(s_1, \ldots, s_n)$.

Cu alte cuvinte, notînd cu S subalgebra polinoamelor simetrice din $R[X_1,\ldots, X_n]$, *unicul morfism de R-algebre* $\psi : R[X_1,\ldots, X_n] \to S$ *cu proprietatea că* $\psi(X_i) = s_i$ *(pentru* $1 \le i \le n$*) este un izomorfism.*

Demonstraţie. Notăm cu $T := \{X_1^{i_1} \ldots X_n^{i_n} \mid (i_1,\ldots,i_n) \in \mathbb{N}^n\}$ mulţimea termilor din $R[X_1,\ldots, X_n]$. Definim o relaţie de ordine pe T (*ordinea lexicografică*): ordonăm total $\{X_1,\ldots, X_n\}$ (de exemplu $X_1 > X_2 > \ldots > X_n$) şi definim $X_1^{i_1} \ldots X_n^{i_n} < X_1^{k_1} \ldots X_n^{k_n} \Leftrightarrow \exists r$, $1 \le r \le n$, astfel încît $i_t = k_t$, $\forall t < r$ şi $i_r < k_r$. Se obţine o relaţie de *ordine strictă* (ireflexivă şi tranzitivă) pe T. De exemplu, avem $1 < X_3^7 < X_2 X_3^2 < X_1 < X_1 X_2^2$. Ca de obicei, notăm cu $\le$ relaţia de ordine (nestrictă) asociată. Această relaţie de ordine este totală[65] şi compatibilă cu înmulţirea, adică, $\forall \lambda, \mu, \nu \in T$, din $\mu \le \nu$ rezultă $\lambda\mu \le \lambda\nu$. Relaţia astfel definită este chiar singura ordine pe T, compatibilă cu înmulţirea, care satisface $X_1 > X_2 > \ldots > X_n$).

Ordinea lexicografică induce o relaţie de preordine[66], notată tot „$\le$", pe mulţimea $\{a\lambda \mid \lambda \in T,\ a \in R,\ a \ne 0\}$ a *monoamelor* din $R[X_1,\ldots, X_n]$, prin $a\lambda \le b\mu \Leftrightarrow \lambda \le \mu$. Demonstrarea afirmaţiilor precedente este un exerciţiu de rutină. Dacă $p \in R[X_1,\ldots, X_n]$, există un unic monom care este cel mai mare monom al lui p (faţă de preordinea lexicografică), numit *monom dominant* al lui p. Îl notăm cu $hm(p)$. Are loc următoarea proprietate:

Dacă $p, q \in R[X_1,\ldots, X_n]$, *astfel încît* $hm(p) = a\lambda$, $hm(q) = b\mu$, *unde* $\lambda, \mu \in T$, $a, b \in R$ *şi* $ab \ne 0$, *atunci* $hm(pq) = hm(p)hm(q) = ab\lambda\mu$.

---

[65] Mai mult, T este o mulţime *bine ordonată* de ordinea lexicografică (orice submulţime nevidă a lui T are un prim element). Se pot face deci demonstraţii prin inducţie după această ordine (cum este demonstraţia de faţă).

[66] Adică o relaţie reflexivă şi tranzitivă, dar nu neapărat antisimetrică.

Într-adevăr, orice monom al lui pq este o sumă de monoame de forma $r\alpha \cdot s\beta$, unde $r\alpha$ este monom al lui p, $s\beta$ este monom al lui q. Dar $\alpha \le \lambda$ şi $\beta \le \mu$, deci $\alpha\beta \le \lambda\beta \le \lambda\mu$. Astfel, $ab\lambda\mu = hm(pq)$.

Fie deci g un polinom simetric şi fie $hm(g) = aX_1^{i_1} \dots X_n^{i_n}$. Atunci $i_1 \ge i_2 \ge \dots \ge i_n$ (dacă $\exists k$ astfel încît $i_k < i_{k+1}$, atunci $aX_1^{i_1} \dots X_k^{i_{k+1}} X_{k+1}^{i_k} \dots X_n^{i_n}$ este monom în g, strict mai mare decît $hm(g)$). Căutăm un polinom p de forma $as_1^{j_1} \dots s_n^{j_n}$ astfel încît $hm(p)$ să fie $hm(g)$. Din proprietatea de mai sus, $hm\left(as_1^{j_1} \dots s_n^{j_n}\right) = aX_1^{j_1}(X_1X_2)^{j_2} \dots (X_1 \dots X_n)^{j_n}$. Acest monom este egal cu $hm(g)$ dacă şi numai dacă $j_1 + \dots + j_n = i_1$, $j_2 + \dots + j_n = i_2$, …, $j_n = i_n$. Rezultă $j_n = i_n$, $j_k = i_k - i_{k+1}$ pentru $1 \le k < n$. Polinomul

$$g_1 := g - as_1^{j_1} \dots s_n^{j_n}$$

este simetric şi are $hm(g_1) < hm(g)$. Dacă $hm(g_1) = 0$, avem $g_1 = 0$ şi am terminat. Dacă $hm(g_1) \ne 0$, aplicăm acelaşi procedeu pentru g_1. Algoritmul se termină după un număr finit de paşi deoarece nu poate exista un şir infinit strict descrescător de termi, conform lemei 4.6. Aceasta încheie demonstrația părții de existență.

Arătăm unicitatea (cu alte cuvinte, $\operatorname{Ker}\psi = 0$). Presupunem că există un polinom nenul $p \in R[X_1, \dots, X_n]$ astfel încît $\psi(p) = p(s_1, \dots, s_n) = 0$. Afirmăm că există un unic monom nenul λ al lui p astfel încît $hm(\psi(p)) = hm(\lambda(s_1, \dots, s_n))$. Dacă $\alpha = X_1^{i_1} \dots X_n^{i_n}$, $\beta = X_1^{j_1} \dots X_n^{j_n} \in T$, cu $\alpha \ne \beta$, atunci:

$$hm(\alpha(s_1, \dots, s_n)) = X_1^{i_1+\dots+i_n} \dots X_n^{i_n} \ne X_1^{j_1+\dots+j_n} \dots X_n^{j_n} = hm(\beta(s_1, \dots, s_n)).$$

Deci $\exists!\ \lambda \ne 0$ monom al lui p astfel încît $hm(\lambda(s_1, \dots, s_n)) = \max\{hm(\alpha(s_1, \dots, s_n)) \mid \alpha$ monom al lui $p\}$. Cum $p(s_1, \dots, s_n) = \sum\{\alpha(s_1, \dots, s_n) \mid \alpha$ monom al lui $p\}$, rezultă că

$hm(p(s_1, \dots, s_n)) = hm(\lambda(s_1, \dots, s_n)) \ne 0$, contradicție cu $p(s_1, \dots, s_n) = 0$. □

Teorema **4.7** se extinde uşor şi la fracții raționale simetrice:

4.8 Corolar. (Teorema fundamentală a fracțiilor raționale simetrice) *Fie R un inel integru şi K corpul său de fracții. Dacă $p, q \in R[X_1, \dots, X_n]$, $q \ne 0$, astfel încît p/q este o fracție rațională simetrică, atunci există polinoamele $f, g \in R[X_1, \dots, X_n]$ astfel încît $\dfrac{p}{q} = \dfrac{f(s_1, \dots, s_n)}{g(s_1, \dots, s_n)}$. Cu alte cuvinte, subcorpul fracțiilor raționale simetrice din corpul $K(X_1, \dots, X_n)$ este $K(s_1, \dots, s_n)$.*

Demonstrație. Dacă q este polinom simetric, atunci p este simetric (ca produs în subcorpul fracțiilor raționale simetrice dintre q şi p/q). Din **4.7** rezultă că $p, q \in R[s_1, \dots, s_n]$. Dacă q nu este simetric, fie $s = \prod_{\sigma \in S_n} \varphi_\sigma(q)$. Atunci s este simetric şi

$$\frac{p}{q} = \frac{p\prod_{\sigma \ne \mathrm{id}} \varphi_\sigma(q)}{s},$$

şi am revenit la primul caz. □

Să exprimăm polinomul simetric $t_m := X^m{}_{;1} + \dots + X^m{}_{;n} \in R[X_1, \dots, X_n]$ ($m \in \mathbb{N}$) în funcție de polinoamele simetrice $s_1, \dots, s_n$. Identitățile următoare permit un calcul recursiv al lui t_m ca polinom de $s_1, \dots, s_n$.

4.9 Propoziție. (Identitățile lui Newton) *În* $R[X_1,\ldots, X_n]$ *are loc relația:*

$$t_m = s_1\, t_{m-1} - s_2\, t_{m-2} + \ldots + (-1)^{m-2} s_{m-1}\, t_1 + (-1)^{m-1} m s_m.$$

Demonstrație. Dacă $m > n$, atunci convenția $s_k = 0$ pentru $k > n$ trunchiază formula de mai sus (sînt numai n termeni).

Fie $r \le n$ și $(a_1, \ldots, a_r)$ un r-uplu de numere naturale cu $a_1 \ge a_2 \ge \ldots \ge a_r$. Notăm cu $s(a_1, \ldots, a_r)$ unicul polinom simetric din $R[X_1,\ldots, X_n]$ cu monomul dominant $X_1^{a_1} X_2^{a_2} \ldots X_r^{a_r}$.

De exemplu, $s(m, 0, \ldots, 0) = X^{m}_{1} + \ldots + X^{m}_{n} = t_m$, $s(1, 1, 0, \ldots, 0) = X_1 X_2 + X_1 X_3 + \ldots = s_2$. Pentru a simplifica notația, punem $1_i := (1, \ldots, 1)$ (1 apare de i ori) și $(a, 1_i) := (a, 1, \ldots, 1)$ (1 apare de i ori); de asemenea, vom omite să scriem un șir de 0: $s(m, 0, \ldots, 0) = s(m)$, $s(1, 1, 0, \ldots, 0) = s(1, 1) = s_2$, $s(1_i, 0, \ldots, 0) = s(1_i) = s_i$. Relațiile următoare se verifică ușor:

$$s_1\, t_{m-1} = t_m + s(m-1, 1)$$
$$s_2\, t_{m-2} = s(m-1, 1) + s(m-2, 1, 1)$$
$$s_3\, t_{m-3} = s(m-2, 1, 1) + s(m-3, 1, 1, 1)$$
$$\ldots$$

Mai general, pentru orice $i \le \min\{m-1, n\}$,

$$s_i\, t_{m-i} = s(m-i+1, 1_i) + s(m-i, 1_i).$$

Dacă $m \le n$ și $i = m-1$, atunci

$$s_{m-1} t_1 = s(2, 1_{m-2}) + m s_m.$$

Dacă $m > n = i$, atunci

$$s_n\, t_{m-n} = s(m-n+1, 1_{n-1}).$$

Identitățile lui Newton rezultă folosind relațiile de mai sus în suma $\sum_{1 \le i < m} (-1)^{i-1} s_i\, t_{m-i}$. □

IV. Aritmetică în inele şi aplicații

Considerăm indispensabilă o bună cunoaştere de către profesorii de matematică a teoriei divizibilității („aritmetica") în $\mathbb{Z}$ şi în inele de forma $K[X]$, cu K corp, această teorie apărînd sub diverse forme pe tot parcursul algebrei studiate în gimnaziu şi liceu. Conceptele şi rezultatele privind divizibilitatea în $\mathbb{Z}$ prezintă multe analogii cu cele din $K[X]$, fenomen care nu este întîmplător, ci este consecința faptului că ambele sînt inele *euclidiene*.

O clasă largă de inele în care se poate dezvolta o teorie a divizibilității care să o urmeze pe cea din $\mathbb{Z}$ este clasa *inelelor integre.* O astfel de generalizare, pe lîngă un interes intrinsec, aduce de multe ori clarificări şi rezultate noi privind chiar divizibilitatea în $\mathbb{Z}$.

Se vor trece în revistă proprietățile generale mai importante ale relației de divizibilitate într-un inel integru. Clase importante de inele (*euclidiene, principale, factoriale*) apar prin abstractizarea unor proprietăți aritmetice ale lui $\mathbb{Z}$. Noțiunile şi rezultatele expuse sînt fundamentale pentru toată algebra, în special pentru teoria algebrică a numerelor şi teoria extinderilor de corpuri.

IV.1 Divizibilitate

Definiția divizibilității în $\mathbb{Z}$ se transpune cuvînt cu cuvînt pentru un inel oarecare R.

1.1 Definiție. Dacă $a, b \in R$, spunem că *a divide b în R* (notație: $a|b$ sau $b \vdots a$) dacă există $c \in R$ astfel încît $b = ac$. Exprimări echivalente: a este *divizor* (uneori se spune şi *factor*) al lui b; b este *multiplu* al lui a; b este *divizibil cu a.*

Faptul că $a|b$ în *R depinde în mod esențial de inelul R*. De exemplu, $2|3$ în $\mathbb{Q}$, dar nu şi în $\mathbb{Z}$! Notăm $a \nmid b$ dacă a nu îl divide pe b.

O teorie relevantă a divizibilității se poate dezvolta în inele cu proprietăți care le apropie cumva de $\mathbb{Z}$. Un set minimal de astfel de proprietăți este: inelul să fie *unitar*, *comutativ* şi *fără divizori ai lui zero* (adică $\forall a, b \in R$, din $ab = 0$ rezultă $a = 0$ sau $b = 0$). Un astfel de inel (notat în continuare cu R) se numeşte *inel integru* sau *domeniu de integritate*, denumire care provine chiar din faptul că proprietățile sale sînt oarecum apropiate de cele din inelul $\mathbb{Z}$ al

întregilor. În această secțiune, *toate inelele vor fi integre, toate corpurile ce intervin vor fi presupuse comutative, iar subinelele care apar vor conține elementul unitate al inelului* (*subinele unitare*). Vom nota cu R^* mulțimea $R \setminus \{0\}$.

1.2 Exemple. Orice corp este inel integru. Teoria divizibilității într-un corp K este trivială: $\forall a$, $b \in K$, are loc $a|b$ (cu excepția cazului cînd $a = 0$ şi $b \neq 0$). Orice subinel al unui inel integru este la rîndul său integru. În particular, orice subinel al unui corp este integru. Dacă R este inel integru, atunci inelul de polinoame cu coeficienți în R, $R[X]$, este integru.

În inele integre se pot simplifica factorii nenuli:

1.3 Propoziție. *Fie R un inel integru şi $a, b, c \in R$, cu $c \neq 0$. Dacă $ac = bc$, atunci $a = b$.*

Demonstrație. Avem $ac = bc \Leftrightarrow ac - bc = 0 \Leftrightarrow (a - b)c = 0$. Nu putem avea $a - b \neq 0$, căci atunci $(a - b)c \neq 0$ din integritatea lui R. Deci $a - b = 0$. □

Proprietățile generale ale relației de divizibilitate sînt binecunoscute (demonstrați-le!):

1.4 Propoziție. *Fie R un inel integru. Atunci:*

a) Pentru orice $a \in R$ are loc $a|a$.

b) Pentru orice $a, b, c \in R$ astfel încît $a|b$ şi $b|c$, rezultă $a|c$.

c) Pentru orice $a \in R$, are loc $a|0$ şi $1|a$.

d) Oricare ar fi $x, y \in R$ şi $a, b, c \in R$ astfel încît $a|b$ şi $a|c$, rezultă $a|(bx + cy)$. □

Relația de divizibilitate este aşadar o relație *reflexivă* şi *tranzitivă*, adică o relație de *preordine* pe R. Relația de echivalență asociată acestei preordini se numeşte relația de *asociere în divizibilitate*:

1.5 Definiție. Spunem că elementele a şi b din R sînt *asociate în divizibilitate* (pe scurt, *asociate*) dacă $a|b$ şi $b|a$. Notație: $a \sim b$. Dacă $d, a \in R$, spunem că d este *divizor propriu al lui a* (sau *divide propriu pe a*) dacă $d|a$ şi d nu este nici inversabil, nici asociat cu a.

Relația "~" definită mai sus este o relație de echivalență pe inelul R şi este deosebit de importantă în studiul aritmeticii lui R: *două elemente asociate în divizibilitate au aceleaşi proprietăți din punct de vedere al divizibilității* (au aceiaşi divizori şi aceiaşi multipli). Mulțimea elementelor asociate cu 1, adică

$$U(R) = \{x \in R \mid \exists\, y \in R \text{ astfel încît } xy = yx = 1\},$$

are un statut special: se numeşte *grupul unităților* lui R, deoarece este grup față de înmulțirea inelului (chiar dacă R nu este comutativ).

1.6 Propoziție. *Fie R un inel integru. Atunci:*

a) Pentru orice $u \in R$, avem: $u \in U(R) \Leftrightarrow u \sim 1 \Leftrightarrow u|a,\ \forall\, a \in R \Leftrightarrow uR = R$.

b) Pentru orice $a, b \in R$, avem: $a \sim b \Leftrightarrow$ există $u \in R$ astfel încît $a = bu$. □

Se justifică denumirea de „unităţi” dată elementelor inversabile: *unităţile se comportă ca şi* 1 (*unitatea inelului*) *faţă de divizibilitate*. De aceea, determinarea grupului unităţilor este importantă în studiul divizibilităţii în R.

1.7 Exemple. a) $U(\mathbb{Z}) = \{-1, 1\}$.

b) Dacă K este un corp, $U(K[X]) = \{ f \in K[X] \mid \text{grad} f = 0\} = K^*$.

Pe mulţimea claselor de echivalenţă în raport cu relaţia „~” de asociere în divizibilitate, relaţia de divizibilitate „ | ” defineşte în mod natural o *relaţie de ordine*. Traducînd noţiunile de margine inferioară (respectiv superioară) a unei submulţimi într-o mulţime ordonată, se ajunge la noţiunile clasice de *cel mai mare divizor comun* şi *cel mai mic multiplu comun*:

1.8 Definiţie. Fie R un inel integru, $n \in \mathbb{N}^*$ şi $a_1, ..., a_n \in R$. Spunem că elementul d din R este un *cel mai mare divizor comun* (pe scurt, *cmmdc*) al elementelor $a_1, ..., a_n$ dacă:

i) $d|a_1, ..., d|a_n$.

ii) Pentru orice $e \in R$ astfel încît $e|a_1, ..., e|a_n$, rezultă $e|d$.

Spunem că elementul m din R este un *cel mai mic multiplu comun* (pe scurt, *cmmmc*) al elementelor $a_1, ..., a_n$ dacă satisface condiţiile:

i') $a_1|m, ..., a_n|m$.

ii') Pentru orice $e \in R$ astfel încît $a_1|e, ..., a_n|e$, rezultă $m|e$.

1.9 Observaţie. Pentru $a_1, ..., a_n \in R$, *dacă există un cmmdc al lor* $d \in R$, *atunci* d *este unic determinat pînă la o asociere în divizibilitate*: dacă şi e este un cmmdc al $a_1, ..., a_n$, atunci $e \sim d$. Aceeaşi observaţie se aplică cmmmc.

În continuare vom nota cu $(a_1, ..., a_n)$ sau cu cmmdc$\{a_1, ..., a_n\}$ un cmmdc al $a_1, ..., a_n$, în cazul cînd acesta există. Scrierea $d = (a_1, ..., a_n)$ semnifică faptul că d este **asociat** cu un cmmdc al $a_1, ..., a_n$. De exemplu, în $\mathbb{Z}$, putem scrie $1 = (1, 2)$ şi $(1, 2) = -1$, dar aceasta nu înseamnă că $1 = -1$ (ci $1 \sim -1$). Spunem că $a_1, ..., a_n$ sînt *relativ prime* (*prime între ele*) dacă şi numai dacă $(a_1, ..., a_n) = 1 \Leftrightarrow$ orice divizor comun al lor este o unitate în R.

Notăm cu $[a_1, ..., a_n]$ sau cu cmmmc$\{a_1, ..., a_n\}$ un cmmmc al $a_1, ..., a_n$, dacă există.

1.10 Observaţie. $\forall a \in R, \exists\ (a, 0) = a$ şi $\exists\ [a, 0] = 0$.

Pentru un inel integru oarecare R şi $x, y \in R$, *nu este garantată existenţa unui cmmdc al lor*. Un inel integru R cu proprietatea că, pentru orice două elemente $x, y \in R$, există un cmmdc al lor, se numeşte *GCD-inel* (*Greatest Common Divisor* înseamnă *cel mai mare divizor comun*).

Iată cîteva proprietăţi elementare generale ale cmmdc şi cmmmc:

1.11 Propoziţie. *Fie R un domeniu de integritate şi* $a_1, ..., a_n, r \in R \setminus\{0\}$.
a) Dacă există $d = (a_1, ..., a_n)$, *atunci* $a_1/d, ..., a_n/d$ *au cmmdc, egal cu* 1.[67]
b) Dacă există $(a_1, ..., a_n) =: d$ *şi există* $(ra_1, ..., ra_n) =: e$, *atunci* $e = rd$, *adică:*

$$(ra_1, ..., ra_n) = r(a_1, ..., a_n).$$

c) Dacă există $[a_1, ..., a_n] = m$ *şi există* $[ra_1, ..., ra_n] =: \mu$, *atunci* $\mu = rm$, *adică:*

$$[ra_1, ..., ra_n] = r[a_1, ..., a_n].$$

Demonstraţie. *a)* Fie $x_i \in R$ astfel încît $a_i = dx_i$, pentru $1 \le i \le n$. Evident, 1 este un divizor comun al elementelor $x_1, ..., x_n$. Dacă $e \in R$ este un alt divizor comun al lor, atunci de este un divizor comun al $a_1, ..., a_n$, deci $de|d$. De aici rezultă că $e|1$.

b) Din $rd|ra_i$, pentru $\forall i$, rezultă că $rd|e$. Fie $u \in R$ cu $e = rdu$. Arătăm că $u|1$. Fie $x_i, y_i \in R$ astfel încît $a_i = dx_i$ şi $ra_i = ey_i$, pentru $1 \le i \le n$. Avem, pentru orice i: $ra_i = rdx_i = rduy_i$. De aici rezultă că u este divizor comun al elementelor x_i, care au cmmdc 1, conform punctului *a)*. □

Rezultatul următor este fundamental în argumentele legate de divizibilitate.

1.12 Corolar. *Fie R un inel integru în care orice două elemente au cmmdc (GCD-inel) şi* $a, b, c \in R$ *cu proprietatea că* $a|bc$ *şi a este prim cu b. Atunci* $a|c$.

Demonstraţie. Din $(a, b) = 1$ şi din propoziţia precedentă, punctul *b)*, rezultă că $(ac, bc) = c$. Cum $a|ac$ şi $a|bc$, din definiţia cmmdc obţinem $a|(ac, bc) = c$. □

1.13 Propoziţie. *Fie R un inel integru astfel încît orice două elemente din R au un cmmdc. Atunci,* $\forall a, b \in R$, *există şi cmmmc al lor* $[a, b]$ *şi avem* $ab = (a, b)\cdot[a, b]$. *Mai mult, pentru orice* $n \in \mathbb{N}^*$, *orice n elemente* $a_1, ..., a_n$ *din R au cmmdc şi cmmmc.*

Demonstraţie. Fie $a, b \in R$ cu $a, b \ne 0$ şi fie $d = (a, b)$. Există $x, y \in R$ cu $a = dx$, $b = dy$. Elementul $m = dxy$ este un multiplu comun al elementelor a şi b. Fie μ un alt multiplu comun al elementelor a şi b. Există $z, t \in R$ astfel încît $\mu = az = dxz$ şi $\mu = bt = dyt$. Deci m divide elementele $\mu y = dxyz$ şi $\mu x = dxyt$. Ştim că există $(\mu x, \mu y)$, deci m divide şi pe $(\mu x, \mu y) = \mu(x, y) = \mu$. Aceasta arată că m este un cmmmc al elementelor a şi b şi că $ab = dm$.

Partea a doua se demonstrează prin inducţie după *n.* (Exerciţiu!). □

Pentru scurtarea exprimării, dacă R este inel integru, notăm

$$R^\circ := \{x \in R \mid x \text{ este nenul şi nu este inversabil}\} = R^* \setminus U(R).$$

Un rol important în divizibilitatea în $\mathbb{Z}$ îl au numerele *prime.* Definiţia elementară uzuală care se dă noţiunii de număr natural prim este „numărul $p > 1$ este prim dacă singurii săi divizori naturali sînt 1 şi p". Aceasta este de fapt noţiunea de element *ireductibil* (se va vedea legătura cu noţiunea de element *prim* definită mai jos).

---

[67] Dacă $d \ne 0$ şi $d|a$, am notat cu a/d unicul element x din R cu proprietatea că $a = dx$.

1.14 Definiţie. Fie R un inel integru şi $p \in R$.

a) Spunem că p este *ireductibil* (*în* R) dacă $p \in R^\circ$ şi p nu are divizori proprii: $\forall d \in R$, $d \mid p \Rightarrow d \sim 1$ sau $d \sim p$.

b) Spunem că p este *prim* (*în* R) dacă $p \in R^\circ$ şi oricare ar fi $a, b \in R$ astfel încît $p|ab$, rezultă $p|a$ sau $p|b$.

Subliniem că *un element prim sau ireductibil este prin definiţie nenul şi neinversabil*. Se demonstrează imediat că *dacă p este prim şi p divide un produs de m elemente din R, atunci p divide unul din factori.*

1.15 Propoziţie. *Fie R un inel integru. Atunci orice element prim este ireductibil.* □

Noţiunile de element prim şi element ireductibil (care sînt echivalente pentru $\mathbb{Z}$, după cum se va vedea) nu coincid în general, dar coincid pentru GCD-inele:

1.16 Propoziţie. *Fie R un GCD-inel. Atunci orice element ireductibil în R este prim în R.*

Demonstraţie. Fie $p \in R$, ireductibil şi $x, y \in R$ astfel încît $p|xy$. Dacă $p \nmid x$, atunci $\exists$ $(p, x) = 1$. Într-adevăr, dacă $d|x$ şi $d|p$, atunci este imposibil ca $d \sim p$ (ar rezulta $p|x$), deci $d \sim 1$. Astfel, $p|xy$ şi p este prim cu x. Corolarul 1.12 asigură că $p|y$. □

Noţiunea de divizibilitate poate fi exprimată în termeni de *ideale*:

1.17 Propoziţie. *Fie R un inel integru,* $n \in \mathbb{N}^*$ *şi* $a, b, x_1, ..., x_n \in R$. *Atunci:*

a) $a|b$ *dacă şi numai dacă* $Ra \supseteq Rb$. [68]

b) $a \sim b$ *dacă şi numai dacă* $Ra = Rb$.

c) a este inversabil dacă şi numai dacă $Ra = R$.

d) a este prim în R dacă şi numai dacă Ra este ideal prim.

e) a este ireductibil în R dacă şi numai dacă Ra este ideal maximal printre idealele principale proprii ale lui R (mai precis: $\forall\ x \in R$ *astfel încît* $Ra \subseteq Rx$, *rezultă* $Ra = Rx$ *sau* $Rx = R$*).*

f) a este divizor comun al $x_1, ..., x_n$ *dacă şi numai dacă* $Rx_1 +...+ Rx_n \subseteq Ra$.

g) Dacă $Rx_1 +... + Rx_n = Ra$, *atunci* $a = (x_1, ..., x_n)$.[69]

h) a este multiplu comun al $x_1, ..., x_n$ *dacă şi numai dacă* $Rx_1 \cap ... \cap Rx_n \supseteq Ra$.

i) $a = [x_1, ..., x_n]$ *dacă şi numai dacă* $Rx_1 \cap ... \cap Rx_n = Ra$.

Demonstraţie. *a)* $a|b \Leftrightarrow$ există $c \in R$ cu $b = ca \Leftrightarrow b \in Ra \Leftrightarrow Rb \subseteq Ra$.

e) Presupunem că a este ireductibil. Dacă Rx este un ideal principal propriu al lui R astfel încît $Ra \subseteq Rx$, rezultă că $x|a$. Cum a nu are divizori proprii, x este asociat cu a sau x este o unitate. Dar x nu poate fi o unitate, căci Rx nu coincide cu inelul R. Astfel $x \sim a$, adică $Rx =$

---

[68] Am notat cu Ra idealul generat de a: $Ra = \{ra \mid r \in R\} = aR$. O altă notaţie pentru Ra este (a).

[69] Reciproca este falsă în general. Pentru un contraexemplu, a se vedea secţiunea „Inele principale”.

Ra. Reciproc, dacă Rx e maximal printre idealele principale proprii, iar $d \in R$ este un divizor al lui a, atunci $Ra \subseteq Rd$, deci $Rd = Ra$ sau $Rd = R$. Aceasta înseamnă că $d \sim a$ sau $d \sim 1$.

g) Din *f)* rezultă că a este divizor comun al $x_1, \ldots, x_n$. Fie $d \in R$ un alt divizor comun al lor. Cum $a \in Rx_1 + \ldots + Rx_n$, $\exists\ c_1, \ldots, c_n \in R$ cu $a = c_1x_1 + \ldots + c_nx_n$. Din $d|x_1, \ldots, d|x_n$ rezultă că $d|a$. □

IV.2 Algoritmul lui Euclid, teorema fundamentală a aritmeticii

Un rol esențial în aritmetica lui $\mathbb{Z}$ îl are *teorema împărțirii cu rest:*

- *Pentru orice $a, b \in \mathbb{Z}$, cu $b \neq 0$, există $q, r \in \mathbb{Z}$, astfel încît $a = bq + r$ şi $|r| < |b|$ sau $r = 0$.*

Această teoremă are drept consecință încă două teoreme fundamentale în $\mathbb{Z}$:

- *Orice ideal al lui $\mathbb{Z}$ este principal* (adică de forma $n\mathbb{Z}$, cu $n \in \mathbb{Z}$).

- *Orice număr întreg nenul şi neinversabil se poate scrie în mod unic ca un produs finit de numere întregi prime (unicitatea fiind înțeleasă pînă la ordinea factorilor şi la o asociere a lor în divizibilitate).* („Teorema fundamentală a aritmeticii" sau „Teorema de descompunere unică în factori primi")

Prin abstractizare, se obțin noțiunile generale de *inel euclidian* (inel în care are loc o teoremă de împărțire cu rest), *inel principal* (în care orice ideal e principal) şi, respectiv, de *inel factorial* (în care este valabilă o teoremă de descompunere unică în factori primi).

2.1 Definiție. Un inel integru R se numeşte *inel euclidian* dacă există o funcție $\varphi : R^* \to \mathbb{N}$ astfel încît: pentru orice $a, b \in R$ cu $b \neq 0$, există $q, r \in R$ cu proprietățile:

$$a = bq + r \text{ şi } (r = 0 \text{ sau } \varphi(r) < \varphi(b)).$$

Vom spune în acest caz că R este inel euclidian *față de funcția* φ.

Proprietatea din definiție este cunoscută sub numele de „teorema împărțirii cu rest în R"; q este numit *cît,* iar r *rest* al împărțirii lui a prin b. Definiția de mai sus e inspirată din teoremele corespunzătoare din inelul $\mathbb{Z}$ (unde rolul funcției φ este jucat de valoarea absolută pe $\mathbb{Z}$), respectiv din inelele $K[X]$ cu K corp, unde φ este funcția grad. Aceste inele constituie şi cele mai importante exemple de inele euclidiene.

2.2 Teoremă (Algoritmul lui Euclid). *Fie R un inel euclidian şi $a, b \in R$, cu $b \neq 0$. Atunci există un cmmdc d al elementelor a şi b. În plus, există (şi se pot determina algoritmic) $u, v \in R$ astfel încît $d = au + bv$.*

Demonstrație. Fie următorul şir de împărțiri cu rest în R ("Algoritmul lui Euclid"):

(1) $\quad a = bq_1 + r_1 \qquad$ cu $r_1 = 0$ sau $\varphi(r_1) < \varphi(b)$;

(2) $\quad b = r_1q_2 + r_2 \qquad$ cu $r_2 = 0$ sau $\varphi(r_2) < \varphi(r_1)$;

(3) $r_1 = r_2q_3 + r_3$ cu $r_3 = 0$ sau $\varphi(r_3) < \varphi(r_2)$;

...

$(n-2)$ $r_{n-4} = r_{n-3}q_{n-2} + r_{n-2}$ cu $r_{n-2} = 0$ sau $\varphi(r_{n-2}) < \varphi(r_{n-2})$;

$(n-1)$ $r_{n-3} = r_{n-2}\,q_{n-1} + r_{n-1}$ cu $r_{n-1} = 0$ sau $\varphi(r_{n-1}) < \varphi(r_{n-2})$;

(n) $r_{n-2} = r_{n-1}\,q_n + r_n$ cu $r_n = 0$.

Existenţa elementelor q_i, $r_i \in R$ cu proprietăţile specificate este asigurată la fiecare pas de definiţia inelului euclidian. Întrucît şirul de numere naturale $\varphi(b)$, $\varphi(r_1)$, $\varphi(r_2)$, ... este strict descrescător, există $n \in \mathbb{N}^*$ cu $r_n = 0$ (algoritmul se termină după un număr finit de paşi). Afirmăm că r_{n-1} („ultimul rest nenul”) este cmmdc al lui a şi b.

Din relaţia (n) avem $r_{n-1}|r_{n-2}$. Relaţia $(n-1)$ arată că $r_{n-1}|\ r_{n-3}$. Folosind în continuare egalităţile $(n-2)$, ..., (3), (2), (1), obţinem (prin inducţie[70]) că $r_{n-1}|b$ şi $r_{n-1}|a$. Fie acum $e \in R$ un divizor comun al elementelor a şi b; atunci e va divide şi pe $r_1 = a - bq_1$. Din relaţia (2), obţinem că $e|r_2 = b - r_1q_2$. Procedînd inductiv, rezultă că $e|r_i$ pentru orice $i < n$, deci $e|r_{n-1}$.

Pentru a obţine scrierea lui $d = r_{n-1}$ sub forma $au + bv$, observăm că $r_1 = a - bq_1$; înlocuind r_1 în (2), obţinem scrierea lui r_2 sub forma $au' + bv'$ ş.a.m.d. Următorul algoritm (numit *algoritmul extins al lui Euclid*) realizează acest lucru (la fiecare pas variabilele u şi v sînt astfel încît ultimul rest găsit este $au + bv$):

***Se dau** : a, b ∈ R.* ***Se obţin** : d = (a, b) ∈ R şi u, v ∈ R astfel încît d = au + bv.*

Începe

Dacă $b = 0$, atunci $d := a$; $u := 1$, $v := 0$; **Stop**.

Altfel $u1 := 1$; $v1 := 0$; $u := 0$; $v := 1$;

Pas 1. Găseşte $q, r \in R$ cu $a = bq + r$ şi $r = 0$ sau $\varphi(r) < \varphi(b)$;

Dacă $r = 0$, atunci pune $d := b$; **Stop.**

Altfel $a := b$; $b := r$; $u1 := u1 - q\cdot u$; $v1 := v1 - q\cdot v$;

$t := u$; $u := u1$; $u1 := t$; *„aici se schimbă între ele cuplurile (u, v) şi*

$t := v$; $v := v1$; $v1 := t$; *(u1, v1)”*

Mergi la *Pas 1.*

Sfîrşit □

2.3 Exemple. a) $\mathbb{Z}$ este inel euclidian faţă de funcţia „valoarea absolută”. Cîtul şi restul unei împărţiri cu rest nu sînt unic determinate: de exemplu, $3 = 2\cdot1 + 1 = 2\cdot2 + (-1)$.

b) Fie K un corp. Inelul $K[X]$ este euclidian faţă de funcţia grad : $K[X] \setminus \{0\} \to \mathbb{N}$, conform teoremei **III.2.1.** $\mathbb{Z}$ şi $K[X]$ sînt cele mai importante exemple de inele euclidiene.

2.4 Definiţie. Un inel integru R se numeşte *inel principal* dacă orice ideal al inelului R este principal. Cu alte cuvinte, oricare ar fi idealul I al lui R, există $a \in R$ astfel încît $I = Ra$.

---

[70] Detaliaţi raţionamentul prin inducţie!

Orice corp K este inel principal (singurele sale ideale sînt 0 şi K). Exemple importante de inele principale sînt furnizate de următoarea propoziție.

2.5 Teoremă. *Orice inel euclidian este inel principal.*

Demonstrație. Fie R un inel euclidian față de funcția φ şi I un ideal nenul al lui R. Fie $\{\varphi(x) \mid x \in I, x \neq 0\}$, submulțime nevidă a lui $\mathbb{N}$. Această submulțime are cel mai mic element, fie acesta $\varphi(a)$, cu $a \in I$, $a \neq 0$ (a poate să nu fie unic determinat). Demonstrăm că $I = Ra$. Evident, $Ra \subseteq I$. Pentru incluziunea inversă, presupunem că există un element $b \in I \setminus Ra$. Din teorema împărțirii cu rest, există $q, r \in R$ cu proprietatea că $b = aq + r$, $r \neq 0$ (căci $b \notin Ra$) şi $\varphi(r) < \varphi(a)$. Cum $a, b \in I$, rezultă că $r \in I$. Însă $\varphi(r) < \varphi(a)$ contrazice alegerea lui a. □

Astfel, dacă K este corp, inelul $K[X]$ este principal; dat un ideal $I \neq 0$ în $K[X]$, un generator al lui I este un polinom $g \in I$ de grad minim printre gradele polinoamelor nenule din I.

Există inele principale care nu sînt euclidiene, dar nu sînt uşor de construit. Un astfel de inel este $\mathbb{Z}\left[\dfrac{1+i\sqrt{19}}{2}\right]$ (vezi ALBU şi ION [1984]).

Inelele principale sînt GCD-inele; oricare ar fi $a, b \in R$, există un cmmdc al lor, anume *orice generator al idealului* $aR + bR$:

2.6 Propoziție. *Fie R un inel principal şi $a, b \in R$. Atunci:*

a) Elementul $d \in R$ este un cmmdc al a şi b dacă şi numai dacă $dR = aR + bR$. În particular, există un cmmdc d al lui a şi b şi există $u, v \in R$ astfel încît $d = au + bv$.

b) Elementul $d \in R$ este un cmmmc al a şi b dacă şi numai dacă $dR = aR \cap bR$.

Demonstrație. *a)* R fiind inel principal, există un generator d al idealului $aR + bR = \{ax + by \mid x, y \in R\}$. Atunci $a, b \in dR$, deci $d|a$, $d|b$. Dacă $e \in R$ astfel încît $e|a$, $e|b$, atunci $e|ax + by$, $\forall x, y \in R$. În particular, $e|d$. Astfel, d este un cmmdc al a şi b. Reciproc, dacă d este un cmmdc al a şi b, rezultă că $d|a$ şi $d|b$, deci $dR \supseteq aR$ şi $dR \supseteq bR$, adică $dR \supseteq aR + bR$. Fie e un generator al idealului $aR + bR$. Cum $e|a$, $e|b$, rezultă că $e|d$, adică $d \in eR = aR + bR$. □

Propoziția de mai sus justifică notația (a, b), folosită atît pentru cmmdc al elementelor a şi b, cît şi pentru idealul generat de a şi b, $aR + bR$.

2.7 Exemplu. Fie R un inel integru care nu e corp şi $r \in R$, nenul, neinversabil. Atunci idealul (r, X) al inelului $R[X]$ nu este principal, deci *inelul* $R[X]$ *nu este principal*. Într-adevăr, presupunem că există $f \in R[X]$ cu $({}^{y}f) = (r, X)$. Atunci rezultă că $f|r$. Trecînd la grade, obținem că grad $f = 0$, adică $f \in R$. Din $f|X$, adică $\exists g \in R[X]$ cu $X = fg$, avem că f este inversabil în R. Deci cmmdc al lui r şi X este 1. Dar idealul generat de r şi X nu conține pe 1, căci altfel ar exista $h, q \in R[X]$ astfel încît $1 = hr + qX$. Punînd $X = 0$ în această egalitate de polinoame, rezultă $1 = h(0)\cdot r$, adică r este inversabil, contradicție.

În particular, inelele $\mathbb{Z}[X]$, $K[X, Y]$ cu K corp *nu sînt principale*. Deci, proprietatea „dacă $a, b \in R$ şi există $d = (a, b)$, atunci $\exists u, v \in R$ astfel încît $d = au + bv$" este falsă în inele care nu

sînt principale. De exemplu, în $K[X, Y]$, avem $(X, Y) = 1$, dar 1 nu se poate scrie ca $X\cdot u + Y\cdot v$, cu $u, v \in K[X, Y]$.

Din Propoziţia 1.16 şi din faptul că inelele principale sînt GCD-inele, rezultă:

2.8 Propoziţie. *Într-un inel principal, noţiunile de element ireductibil şi element prim coincid.* □

2.9 Corolar. *Într-un inel principal R, idealele prime nenule sînt ideale maximale. Orice ideal maximal este de forma pR, unde p este ireductibil în R. Un element $p \in R$ este ireductibil dacă şi numai dacă pR este ideal maximal.*

Demonstraţie. Este suficient să observăm că orice ideal prim nenul este principal, generat cu necesitate de un element prim p (Propoziţia 1.17.*d)*). Elementul p este ireductibil, deci (Propoziţia 1.17.*e)*) idealul pR este maximal. Celelalte afirmaţii sînt evidente, ţinînd cont de propoziţia citată şi de faptul că R este principal. □

Cazul particular $R = \mathbb{Z}$ al Propoziţiei următoare este cunoscut sub numele de „Teorema fundamentală a aritmeticii". Reamintim că $R° = \{x \in R \mid x$ este nenul şi nu este inversabil$\}$.

2.10 Teoremă. *Fie R un inel principal. Atunci orice element nenul şi neinversabil din R se poate scrie ca un produs finit de elemente prime.*

Demonstraţie. Presupunem că există $r_0 \in R°$ astfel încît r nu se poate scrie ca un produs finit de elemente prime (sau, echivalent, ireductibile, căci R este principal). În particular, r_0 nu este ireductibil, deci $r_0 = r_1s_1$, cu $r_1, s_1 \in R°$, neasociate cu r_0. Dacă r_1 şi s_1 sînt produse finite de ireductibile, atunci r_0 este produs de ireductibile, fals. Deci măcar unul dintre ele (fie acesta r_1) nu se scrie ca produs de elemente ireductibile. Înlocuind în raţionamentul de mai sus pe r_0 cu r_1, rezultă că există $r_2 \in R°$, $r_2|r_1$, $r_2 \not\sim r_1$. Procedînd recursiv, rezultă existenţa unui şir $(r_n)_{n\geq 0}$ de elemente din R, astfel încît pentru orice $n \in \mathbb{N}$, r_{n+1} este un divizor propriu al lui r_n. Altfel spus, am obţinut un şir infinit strict crescător de ideale $r_0R \subset r_1R \subset \ldots \subset r_nR \subset \ldots$. Dar acest lucru este imposibil într-un inel principal, după cum arată lema următoare.

2.11 Lemă. *Fie R un inel principal şi $(r_n)_{n\geq 0}$ un şir de elemente din R astfel încît $r_nR \subseteq r_{n+1}R$, pentru orice $n \in \mathbb{N}$. Atunci există $m \in \mathbb{N}$ astfel încît $r_mR = r_{m+i}R$, pentru orice $i \in \mathbb{N}$. (Orice şir ascendent de ideale este staţionar).*

Demonstraţie. Fie I reuniunea idealelor r_nR, $n \in \mathbb{N}$. Se arată imediat că I este ideal în R. Cum R este principal, există $a \in R$ astfel încît $I = aR$. Întrucît $a \in I$, există $m \in \mathbb{N}$ astfel încît $a \in r_mR$, adică $aR = r_mR$. Deci $r_mR = aR = I = r_{m+i}R$, $\forall i \in \mathbb{N}$. □

2.12 Definiție. Un inel integru R cu proprietatea că orice element nenul şi neinversabil se scrie ca un produs finit[71] de elemente prime se numeşte *inel factorial* sau *inel cu descompunere unică în factori (primi)*. În literatura anglo-saxonă, astfel de inele sînt numite *Unique Factorization Domains* (*UFD*).

Din teorema 2.10 rezultă că inelele principale (deci şi cele euclidiene) sînt factoriale. Orice corp este inel factorial, căci nu are elemente nenule şi neinversabile.

2.13 Propoziție. *Într-un inel factorial R orice element ireductibil este prim.*

Demonstrație. Fie p ireductibil. Cum $p \in R^\circ$, p este un produs de elemente prime. Acest produs nu poate avea decît un factor, altfel elementul p ar admite divizori proprii. Cu alte cuvinte, p este el însuşi prim. □

Propoziția următoare justifică şi precizează denumirea de *inele cu descompunere unică în factori* primi, care se mai dă inelelor factoriale.

2.14 Propoziție. *Fie R un inel integru şi $r \in R^\circ$. Dacă r admite o descompunere în factori primi, atunci această descompunere este unic determinată pînă la o ordine a factorilor şi pînă la o asociere a acestora în divizibilitate. Mai precis, dacă $r = p_1 \ldots p_n = q_1 \ldots q_m$ sînt două scrieri ale lui r ca produse de elemente prime, atunci $m = n$ şi există o permutare σ a mulțimii $\{1, \ldots, n\}$ astfel încît p_i să fie asociat în divizibilitate cu $q_{\sigma(i)}$, $\forall i \in \{1, \ldots, n\}$.*

Demonstrație. Demonstrăm afirmația propoziției prin inducție după n.

Dacă $n = 1$, atunci $r = p_1 = q_1 \ldots q_m$, cu $p_1, q_1, \ldots, q_m$ prime. Deci r este prim şi divide $q_1 \ldots q_m$; rezultă că r divide unul din factori, fie acesta (după o eventuală renumerotare) q_1. Întrucît q_1 este ireductibil, rezultă că $r \sim q_1$, adică $r = q_1 u$, cu u inversabil. Dacă $m \geq 2$, din egalitatea $q_1 u = q_1 q_2 \ldots q_m$, obținem $q_2 \ldots q_m = 1$, adică $q_2, \ldots, q_m$ sînt inversabile, contradicție. Deci $m = 1$.

Fie $n > 1$ şi presupunem că afirmația este adevărată pentru orice $x \in R^\circ$ care admite o descompunere în factori primi cu mai puțin de n factori. Fie $r \in R$ cu $r = p_1 \ldots p_n = q_1 \ldots q_m$, cu $p_1, \ldots, p_n, q_1, \ldots, q_m$ prime. Din faptul că p_n este prim, rezultă că există $i \in \{1, \ldots, n\}$ astfel încît $p_n | q_i$. Cum q_i este ireductibil, rezultă că $p_n \sim q_i$, adică $v p_n = q_i$, cu v inversabil. Simplificînd prin p_n, obținem $p_1 \ldots p_{n-1} = v q_1 \ldots q_{i-1} q_{i+1} \ldots q_m$. Putem acum aplica ipoteza de inducție pentru produsul $p_1 \ldots p_{n-1}$ şi se obține că $n - 1 = m - 1$ şi $p_1, \ldots, p_{n-1}$ sînt asociate cu $q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_m$, eventual în altă ordine. □

2.15 Teoremă. *Fie R un inel integru. Următoarele afirmații sînt echivalente:*

a) R este inel factorial.

[71] Un astfel de produs se mai numeşte *descompunere în factori* a elementului respectiv. Produsele pot avea şi un singur factor (adică elementul însuşi este prim).

b) Orice element din R° este un produs de elemente ireductibile şi orice element ireductibil este prim.

c) Orice element din R° are o descompunere în factori ireductibili, unică pînă la ordinea factorilor şi pînă la o asociere în divizibilitate a acestora.

d) Orice element din R° are o descompunere în factori ireductibili şi orice două elemente au un cmmdc.

Demonstraţie. *a)⇒b)* Evident, din Propoziţia 2.13.

b)⇒c) Rezultă din Propoziţia 2.14.

c)⇒d) Fie $a, b \in R°$ (dacă a, b sînt nule sau inversabile, există evident un cmmdc al lor). Pentru a găsi un cmmdc al elementelor a şi b, se foloseşte procedeul de determinare a cmmdc învăţat în gimnaziu : „se iau factorii primi comuni la puterea cea mai mică”. Trebuie însă puţină atenţie la asocierea în divizibilitate. Fie P un sistem de reprezentanţi ai claselor de echivalenţă ale elementelor ireductibile din R (în raport cu relaţia de asociere în divizibilitate). Aceasta înseamnă că orice element ireductibil din R este asociat cu exact un element din P. Atunci există şi sînt unic determinate $p_1, \ldots, p_n \in P$, distincte, $s_1, \ldots, s_n, t_1, \ldots, t_n \in \mathbb{N}$, $u, v \in U(R)$ astfel încît $a = p_1^{s_1} \ldots p_n^{s_n} u$ şi $b = p_1^{t_1} \ldots p_n^{t_n} v$. Faptul că aceste elemente sînt unic determinate rezultă imediat din unicitatea descompunerilor în R. Fie $r_i = \min(s_i, t_i)$ şi definim $d = p_1^{r_1} \ldots p_n^{r_n}$. Se observă că $d|a$, $d|b$. Dacă $e|a$, $e|b$, atunci orice factor ireductibil $c \in P$ care îl divide pe e divide pe a şi pe b. Aceasta implică $c \in \{p_1, \ldots, p_n\}$, căci altfel a (sau b) ar avea două descompuneri în factori ireductibili, dintre care una îl conţine pe c, iar cealaltă nu, ceea ce contrazice unicitatea descompunerilor. Deci e este de forma $p_1^{w_1} \ldots p_n^{w_n} q$, cu $w_1, \ldots, w_n \in \mathbb{N}$, $q \in U(R)$. Din $e|a$ rezultă că $w_i \le s_i$, iar din $e|b$ rezultă că $w_i \le t_i$, $i = \overline{1,n}$. Deci $w_i \le r_i$ şi $e|d$.

d)⇒a) Prop. 1.16 asigură că orice element ireductibil este prim, căci R este GCD-inel. Implicaţia e acum evidentă. □

Într-un inel factorial R orice două elemente a şi b au un cmmmc, produsul „factorilor primi comuni şi necomuni la puterea cea mai mare”. Cu notaţiile din demonstraţie, se defineşte $q_i = \max(s_i, t_i)$, iar elementul $m = p_1^{q_1} \ldots p_n^{q_n}$ este un cmmmc al lui a şi b. Demonstraţi!

Proprietatea următoare apare adesea în raţionamentele privind divizibilitatea:

2.16 Propoziţie. *Fie R un inel factorial, $n \in \mathbb{N}^*$ şi $a, b_1, \ldots, b_n \in R$. Dacă a este prim cu orice b_i, $1 \le i \le n$, atunci a este prim cu produsul $b_1 \ldots b_n$.*

Demonstraţie. Vom arăta că nu există nici un element prim p care să dividă atît pe a cît şi produsul $b_1 \ldots b_n$. Dacă p este un astfel de element, atunci există j, $1 \le j \le n$ astfel încît $p|b_j$. Cum $p|a$, rezultă că $p|(a, b_j) = 1$. Deci p este inversabil, contradicţie. □

Vom demonstra următorul rezultat important privitor la inelele de polinoame:

2.17 Teoremă. *Dacă R este inel factorial, atunci inelul de polinoame $R[X]$ este inel factorial.*

Pentru demonstrație sînt necesare cîteva noțiuni şi rezultate, care au şi un interes de sine stătător.

2.18 Definiție. Fie R un inel factorial şi $f = a_0 + a_1X + \ldots + a_nX^n \in R[X]$. Cmmdc al coeficienților $a_0, a_1, \ldots, a_n$ este numit *conținutul* polinomului f, notat $c(f)$. Un polinom cu conținutul asociat cu 1 se numeşte polinom *primitiv*.

Polinomul f este primitiv dacă şi numai dacă nu există p prim în R astfel încît p să dividă toți coeficienții lui f. Orice polinom $f \in R[X]$ se poate scrie sub forma $f = c(f)\cdot f'$, unde f' este polinom primitiv. Reciproc, dacă $f = a\cdot f'$, cu $a \in R$ şi f' primitiv, atunci $a = c(f)$.

2.19 Propoziție. *a) Fie R un inel integru. Dacă p este un element prim în R, atunci p este prim şi în $R[X]$.*

b) (Lema lui Gauss) Fie R un inel factorial şi $f, g \in R[X]$ două polinoame primitive. Atunci şi produsul fg este polinom primitiv.

c) Fie R un inel factorial şi $f, g \in R[X]$. Atunci $c(fg) = c(f)\cdot c(g)$.

Demonstrație. *a)* Remarcăm mai întîi că p divide un polinom în $R[X]$ dacă şi numai dacă p divide toți coeficienții polinomului. Fie $f = a_0 + a_1X + \ldots + a_nX^n$, $g = b_0 + b_1X + \ldots + b_mX^m \in R[X]$ astfel încît $p \nmid f$ şi $p \nmid g$. Să demonstrăm că $p \nmid fg$. Din $p \nmid f$ rezultă că există i, $0 \le i \le n$, astfel încît $p \nmid a_i$. Alegem i minim cu această proprietate. La fel, fie j minim astfel încît $p \nmid b_j$. Atunci coeficientul lui X^{i+j} în produsul fg este

$$\sum_{k+l=i+j} a_k b_l$$

În această sumă, a_ib_j nu este divizibil cu p, iar ceilalți termeni sînt divizibili cu p, fiind produse de doi factori dintre care măcar unul este divizibil cu p. Deci coeficientul lui X^{i+j} nu este divizibil cu p şi nici polinomul fg nu este.

b) Dacă fg nu ar fi polinom primitiv, atunci ar exista $p \in R$, prim, astfel încît $p | fg$. Din punctul precedent obținem că $p | f$ sau $p | g$, contradicție.

c) Fie $f = c(f)\cdot f'$, $g = c(g)\cdot g'$, unde f' şi g' sînt polinoame primitive. Atunci

$$fg = c(f)c(g)\cdot f'\cdot g',$$

cu $f'g'$ polinom primitiv din *b)*. Este clar acum că $c(fg) = c(f)c(g)$. □

2.20 Propoziție. *Fie R un inel factorial, K corpul său de fracții şi $f \in R[X]$, $\text{grad}\, f \ge 1$. Atunci f este ireductibil în $R[X]$ dacă şi numai dacă f este primitiv şi este ireductibil în $K[X]$.*

Demonstrație. Fie f ireductibil în $R[X]$. Atunci e clar că f este primitiv. Să arătăm că f este ireductibil în $K[X]$. Dacă $f = gh$, cu $g, h \in K[X]$, atunci, înmulțind cu cmmmc al numitorilor coeficienților polinoamelor g şi h, obținem o relație de forma $af = g_1h_1$, cu $g_1, h_1 \in R[X]$, $a \in R$. Trecînd la conținutul polinoamelor, avem $a = c(g_1)c(h_1)$, căci $c(f) = 1$. Fie $g_1 = c(g_1)\cdot g_2$, $h_1 = c(h_1)\cdot h_2$, unde g_2, h_2 sînt polinoame primitive. Deci, $af = c(g_1)\cdot c(h_1)\cdot g_2\cdot h_2$; simplificînd prin a, obținem $f = g_2h_2$. Ireductibilitatea lui f implică $\text{grad}\, g_2 = 0$ (de exemplu). Cum $\text{grad}\, g = \text{grad}\, g_1 = \text{grad}\, g_2$, rezultă $\text{grad}\, g = 0$.

Reciproc, dacă $f \in R[X]$ este ireductibil în $K[X]$, nu are divizori proprii (de grad ≥ 1) în $K[X]$; cu atît mai mult nu are divizori de grad ≥ 1 în $R[X]$. Dacă f este şi primitiv, nu are nici factori de grad 0 neinversabili, deci este ireductibil în $R[X]$. □

Propoziţia are o importanţă practică: studiul ireductibilităţii unui polinom în $K[X]$ se reduce la ireductibilitatea în $R[X]$, în principiu mai abordabilă.

Demonstraţia teoremei 2.17. Arătăm mai întîi că în $R[X]$ orice ireductibil este prim: fie $f \in R[X]$, ireductibil. Dacă $f \mid gh$, cu $g, h \in R[X]$, din faptul că f este ireductibil în $K[X]$ (deci şi prim în $K[X]$) rezultă că $f \mid g$ sau $f \mid h$ în $K[X]$. Presupunem că $f \mid g$ în $K[X]$; există deci $a \in R$, $q \in R[X]$ astfel încît $ag = fq$. Trecînd la conţinutul polinoamelor, avem $a \cdot c(g) = c(q)$. Scriind că $q = c(q) \cdot q'$, $g = c(g) \cdot g'$, cu q', g' primitive în $R[X]$, obţinem $ac(g) \cdot g' = f c(q) \cdot q'$; simplificînd prin $c(q) = ac(g)$, rezultă $g' = fq'$, adică $f \mid g$ în $R[X]$.

Rămîne de arătat că orice f nenul şi neinversabil din $R[X]$ este un produs de ireductibile. Vom demonstra aceasta prin inducţie după grad f. Dacă grad $f = 0$, atunci $f \in R^{\circ}$ şi deci are o descompunere în factori ireductibili în R, care rămîn ireductibili în $R[X]$. Dacă grad $f > 0$, fie $f = c(f)f'$, cu f' primitiv; este suficient să găsim o descompunere pentru f'. Dacă f' este ireductibil, am terminat; dacă nu, f' are un divizor propriu în $R[X]$, care este un polinom de grad strict mai mic decît grad f (f' nu are divizori proprii în R, căci este primitiv). În concluzie, $f' = gh$, cu $g, h \in R[X]$, de grade strict mai mici decît grad f. Aplicînd ipoteza de inducţie pentru g şi h, rezultă că f' este un produs de factori ireductibili în $R[X]$. □

Deci *inelele* $\mathbb{Z}[X]$, $\mathbb{Z}[X_1, \ldots, X_n]$, $K[X_1, \ldots, X_n]$ *cu K corp sînt inele factoriale.*

IV.3 Ireductibilitate în inele polinomiale

Fiind dat un inel integru (sau un corp) R, problema deciderii ireductibilităţii unui polinom în inelul de polinoame $R[X]$ nebanală şi adesea deosebit de importantă. De aici rezultă utilitatea cunoaşterii unui arsenal cît mai bogat de criterii de ireductibilitate. Mai întîi determinăm toate polinoamele *inversabile* în $R[X]$.

3.1 Propoziţie. *Fie R un inel integru. Atunci* $U(R[X]) = U(R)$. *În particular, pentru K corp,* $U(K[X]) = K^*$. □

3.2 Observaţie. Dacă R este inel integru şi $f \in R[X]$ este un polinom *unitar reductibil*, atunci există o descompunere a lui f de forma $f = gh$, cu g, $h \in R[X]$ *unitare*, de grade > 1. (demonstraţi!). Această observaţie simplă este utilă în investigarea ireductibilităţii polinoamelor.

Dacă R este inel care nu e corp, inelul $R[X]$ nu este principal, deci cu atît mai mult nu este euclidian (nu are loc teorema împărțirii cu rest în $R[X]$). Totuşi, dacă $f, g \in R[X]$, iar g are coeficientul dominant *inversabil* în R, se poate face „împărțirea cu rest” a lui f la g:

3.3 Propoziție. (teorema împărțirii întregi) *Fie R un inel şi $f, g \in R[X]$. Dacă coeficientul dominant al lui g este inversabil în R, atunci există $q, r \in R[X]$ astfel încît $f = gq + r$, cu $r = 0$ sau* $\operatorname{grad} r < \operatorname{grad} f$.

Demonstrație. Se aplică exact aceeaşi idee ca la demonstrația teorremei împărțirii cu rest în $K[X]$, cu K corp. □

3.4 Corolar (teorema lui Bézout)**.** *Fie R un inel integru, $f \in R[X]$ şi $a \in R$. Atunci a este rădăcină a lui f dacă şi numai dacă polinomul $X - a$ îl divide pe f în $R[X]$.*

Demonstrație. Există $q, r \in R[X]$ astfel încît $f = (X - a)q + r$, unde $\operatorname{grad} r = 0$ sau $r = 0$. Observăm că $(X - a) | f$ dacă şi numai dacă $r = 0$. Din egalitatea $f(a) = (a - a)q(a) + r(a) = r$, deducem că $f(a) = 0$ echivalează cu $r = 0$. □

Deci, *dacă* $\operatorname{grad} f \geq 2$ *şi f are o rădăcină $a \in R$, atunci f este reductibil în* $R[X]$ (fiind divizibil cu $X - a$). Reciproca este falsă: polinomul $(X^2 + 1)^2$ nu are rădăcini în $\mathbb{Q}$, dar este evident reductibil în $\mathbb{Q}[X]$. Are loc o reciprocă „parțială”:

3.5 Propoziție. *Fie K un corp. Atunci un polinom f de grad 2 sau 3 din $K[X]$ este ireductibil dacă şi numai dacă nu are rădăcini în K. În particular, dacă R este inel factorial, un polinom primitiv de grad 2 sau 3 din $R[X]$ este ireductibil în $R[X]$ dacă şi numai dacă nu are rădăcini în K.*

Demonstrație. Fie $f \in K[X]$, reductibil şi de grad 2 sau 3. Din examinarea gradelor într-o descompunere a lui f, rezultă că are un factor de grad 1, care are o rădăcină în K. Restul rezultă din echivalența „f este ireductibil în $R[X]$ dacă şi numai dacă f este primitiv şi ireductibil în $K[X]$”. □

Criteriul de mai sus trebuie aplicat cu precauție pentru stabilirea ireductibilității polinoamelor cu coeficienți într-un *inel* integru (mai ales dacă nu e factorial):

3.6 Exemple. a) Polinomul $f = (2X + 1)^2$ este evident reductibil în $\mathbb{Z}[X]$, dar nu are rădăcini în $\mathbb{Z}$. Însă f are rădăcini în corpul de fracții al lui $\mathbb{Z}$, $\mathbb{Q}$.

b) Fie $R = \{a + 2bi \mid a, b \in \mathbb{Z}\}$. Se verifică imediat că R este subinel integru al lui $\mathbb{Z}[i]$. Polinomul $X^2 + 1$ este ireductibil în $R[X]$ (demonstrați!), dar are rădăcinile $i, -i$ în corpul de fracții al lui R, $\mathbb{Q}[i]$. Aceasta arată că existența rădăcinilor unui polinom de grad 2 sau 3 din $R[X]$ în corpul de fracții al lui R nu implică în general reductibilitatea polinomului în $R[X]$.

În cazul corpurilor $\mathbb{C}$ şi $\mathbb{R}$, ideile simple de mai sus, cuplate cu Teorema fundamentală a algebrei, furnizează lista *tuturor* polinoamelelor ireductibile peste aceste corpuri:

3.7 Propoziţie. *a) Polinomul* $f \in \mathbb{C}[X]$ *este ireductibil dacă şi numai dacă este polinom de grad I.*

b) Polinomul $f \in \mathbb{R}[X]$ *este ireductibil dacă şi numai dacă: sau este polinom de grad I, sau este de grad II* (*de forma* $aX^2 + bX + c$, *cu* $a \neq 0$) *şi discriminantul său* $b^2 - 4ac$ *este negativ.*

Demonstraţie. *a)* Evident, orice polinom de grad I este ireductibil. Reciproc, dacă $f \in \mathbb{C}[X]$ şi $\text{grad} f > 1$, atunci f are o rădăcină $z \in \mathbb{C}$ (conform teoremei fundamentale a algebrei), deci f nu poate fi ireductibil.

b) Exerciţiu. □

Pentru găsirea rădăcinilor unui polinom este util următorul criteriu (vezi şi Exerc. 13).

3.8 Propoziţie. *Fie R un inel factorial, K corpul său de fracţii şi* $f = a_0 + \dots + a_nX^n \in R[X]$. *Dacă* $p/q \in K$ *este o rădăcină a lui f, cu* $p, q \in R$, $(p, q) = 1$, *atunci* $p|a_0$ *şi* $q|a_n$.

Demonstraţie. Scriind că p/q este rădăcină a lui f şi înmulţind cu q^n, avem

$$-a_0q^n = a_1pq^{n-1} + \dots + a_np^n,$$

deci $p|a_0q^n$. Cum $(p, q) = 1$, avem şi $(p, q^n) = 1$ (R este factorial) şi deci $p|a_0$. Analog se demonstrează că $q|a_n$. □

3.9 Exemplu. Fie $f = X^3 - X + 2 \in \mathbb{Z}[X]$. Dacă $p/q \in \mathbb{Q}$ este rădăcină a lui f, $(p, q) = 1$, atunci $p|2$ şi $q|1$. Rădăcinile raţionale ale lui f (dacă există) se găsesc aşadar printre elementele mulţimii $\{1, -1, 2, -2\}$. Prin testare directă, obţinem că nici unul din aceste elemente nu este rădăcină. Deci f nu are rădăcini raţionale. Cum f este de grad 3, rezultă că este ireductibil în $\mathbb{Q}[X]$ (şi în $\mathbb{Z}[X]$, fiind primitiv).

Fie R un inel. Teorema lui Bézout afirmă că polinomul $f \in R[X]$ are rădăcina $a \in R$ dacă şi numai dacă $X - a$ divide f în $R[X]$. Este aşadar naturală considerarea următoarei definiţii:

3.10 Definiţie. Fie R un inel integru, $f \in R[X]$ un polinom nenul, $a \in R$ o rădăcină a lui f şi $n \in \mathbb{N}$. Spunem că a este *rădăcină multiplă de ordin n a lui f* dacă $(X - a)^n \mid f$ şi $(X - a)^{n+1} \nmid f$. Numărul natural n se numeşte *ordinul de multiplicitate al rădăcinii a*. Dacă $n = 1$, a se numeşte *rădăcină simplă*, dacă $n = 2, 3, \dots$, a se numeşte *rădăcină dublă*, *triplă*… . Atunci cînd se numără rădăcinile unui polinom, *se numără fiecare rădăcină de atîtea ori cît este ordinul său de multiplicitate*.

3.11 Propoziţie. *Fie R un inel factorial şi* $f \in R[X]$ *un polinom nenul. Dacă* $a_1, \dots, a_n \in R$ *sînt rădăcini distincte ale lui f, de ordine de multiplicitate* $m_1, \dots, m_n$, *atunci f se divide cu* $(X - a_1)^{m_1} \dots (X - a_n)^{m_n}$ *în* $R[X]$.

Demonstraţie. Prin inducţie după n. Dacă $n = 1$, afirmaţia rezultă din definiţie. Presupunem afirmaţia adevărată pentru $n - 1$ şi fie f ca în enunţ. Din ipoteza de inducţie, $f = (X - a_1)^{m_1} \dots (X - a_{n-1})^{m_{n-1}} g$, cu $g \in R[X]$. Polinoamele $X - a_i$, cu $1 \leq i \leq n$, sînt

ireductibile şi neasociate două cîte două; deci $(X-a_1)^{m_1}$, …, $(X-a_n)^{m_n}$ sînt două cîte două relativ prime. Din Prop. IV.2.16 rezultă că $(X-a_n)^{m_n}$ este prim cu produsul $(X-a_1)^{m_1}\dots(X-a_{n-1})^{m_{n-1}}$. Dar $(X-a_n)^{m_n}$ divide pe $(X-a_1)^{m_1}\dots(X-a_{n-1})^{m_{n-1}}g$, deci $(X-a_n)^{m_n} \mid g$. □

3.12 Observație. În $\mathbb{C}[X]$, *orice* polinom se scrie în mod unic sub forma $b(X_1-a_1)^{m_1}\dots(X_n-a_n)^{m_n}$, unde $a_1, \dots, a_n \in \mathbb{C}$ sînt distincte două cîte două (sînt rădăcinile polinomului), iar b este coeficientul său dominant. Acest lucru rezultă din faptul că $\mathbb{C}[X]$ este inel factorial (orice polinom se scrie ca un produs de polinoame ireductibile), ținînd cont de lista polinoamelor ireductibile din $\mathbb{Z}[X]$. Care este forma generală a unei descompuneri în factori ireductibili a unui polinim din $\mathbb{R}[X]$?

3.13 Corolar. *Fie R un inel integru şi $f \in R[X]$,* grad $f = n$. *Atunci f are cel mult n rădăcini în R.*

Demonstrație. Fie K corpul de fracții al lui R. Interpretînd f ca polinom în $K[X]$, afirmația decurge din propoziția precedentă. □

Vom da un criteriu pentru a decide dacă un polinom are rădăcini multiple, folosind noțiunea de *derivată formală* a unui polinom.

3.14 Definiție. Fie R un inel comutativ unitar şi $f = a_0 + a_1X + \dots + a_nX^n \in R[X]$. Numim *derivată (formală)* a polinomului f polinomul

$$\mathrm{d}f := a_1 + 2a_2X + \dots + na_nX^{n-1}.$$

Se mai foloseşte notația $\mathrm{d}f = f'$ sau $\mathrm{d}f = f^{(1)}$.

Un calcul direct arată că derivata formală are proprietățile uzuale ale derivatei cunoscute din Analiză:

$$(f+g)' = f' + g',\quad (af)' = af',\quad (fg)' = f'g + fg',\quad \forall a \in R, \forall f, g \in R[X].$$

Compunerea morfismului d cu el însuşi de n ori ($n \in \mathbb{N}^*$) se notează d^n; $\mathrm{d}^n : R[X] \to R[X]$. Avem deci $\mathrm{d}^n = \mathrm{d}\circ\mathrm{d}^{n-1}$, $\forall n \in \mathbb{N}^*$, cu convenția că $\mathrm{d}^0 = \mathrm{id}$. Mai notăm $\mathrm{d}^n f = f^{(n)}$, $\forall f \in R[X]$.

3.15 Propoziție. *Fie R un inel integru, $f \in R[X]$ un polinom de grad $n > 0$ şi $\alpha \in R$.*

a) Există şi sînt unice elementele $b_0, \dots, b_n \in R$ astfel încît $f = \sum_{0\le i\le n} b_i(X-\alpha)^i$.

b) Dacă α este rădăcină multiplă de ordin m ($m \in \mathbb{N}^*$) a polinomului f, atunci $f^{(i)}(\alpha) = 0$, *pentru orice $i \in \{0, \dots, m-1\}$.*

c) Dacă $f(\alpha) = f'(\alpha) = 0$, *atunci α este rădăcină multiplă a lui f (de multiplicitate cel puțin* 2*).*

Demonstrație. a) Prin inducție după grad f. Dacă $f = a_0 + a_1X$, atunci $f = a_0 + a_1\alpha + a_1(X-\alpha)$. Dacă grad $f = n > 1$, aplicînd teorema împărțirii întregi (IV.3.3), obținem

$f = (X - \alpha)g + b_0$, cu $b_0 \in R$ şi $g \in R[X]$, grad $g = n - 1$. Scriind pe g sub forma dată de ipoteza de inducţie şi înlocuind în relaţia precedentă, se obţine rezultatul.

Unicitatea scrierii este echivalentă cu R-liniara independenţă a mulţimii de polinoame $\{(X - \alpha)^i \mid i \in \mathbb{N}\}$ în $R[X]$, uşor de demonstrat.

b) Din relaţia dedusă la punctul a), rezultă că $(X - \alpha)^m \mid f$ dacă şi numai dacă $b_0, b_1, \ldots, b_{m-1}$ sînt nuli. Pe de altă parte, se demonstrează uşor că $f^{(i)}(\alpha) = i!b_i$, $\forall i \in \{0, \ldots, n\}$. De aici rezultă că $f^{(i)}(\alpha) = 0$, $\forall i \in \{0, \ldots, m-1\}$.

c) Din cele demonstrate pînă acum, obţinem că $f(\alpha) = b_0 = 0$ şi $f'(\alpha) = b_1 = 0$. Deci $(X - \alpha)^2 \mid f$. □

În cazul polinoamelor cu coeficienţi într-un corp K, un element α dintr-o extindere E a lui K este rădăcină multiplă a polinomului f dacă şi numai dacă este simultan rădăcină a polinomului şi a derivatei sale, adică $(X - \alpha) \mid f$ şi $(X - \alpha) \mid f'$. Aceasta implică faptul că cmmdc al lui f şi f' în $E[X]$ este de grad ≥ 1. *Însă cmmdc a două polinoame se obţine cu algoritmul lui Euclid şi nu depinde de corpul considerat*: *dacă $K \subseteq L$ este o extindere de corpuri, iar f, $g \in K[X]$, atunci $(f, g)_{K[X]} = (f, g)_{L[X]}$*. În concluzie:

3.16 Propoziţie. *Fie K un corp şi $f \in K[X]$. Atunci f are rădăcini multiple dacă şi numai dacă f şi f' nu sînt prime între ele.* □

Astfel, se poate decide dacă un polinom are rădăcini multiple *fără a cunoaşte rădăcinile*.

Iată o aplicaţie importantă a teoremei împărţirii cu rest în inele de polinoame: teorema de descompunere a unei funcţii raţionale în sumă de funcţii raţionale simple, instrument esenţial pentru găsirea primitivei unei funcţii raţionale.

3.17 Teoremă (Descompunerea unei funcţii raţionale în sumă de funcţii raţionale simple). *Fie P, $Q \in \mathbb{R}[X]$, cu $Q \neq 0$. Fie descompunerea lui Q în factori ireductibili în $\mathbb{R}[X]$:*

$$Q = (X - a_1)^{\alpha_1} \ldots (X - a_k)^{\alpha_k} \left(X^2 + b_1 X + c_1\right)^{\beta_1} \ldots \left(X^2 + b_r X + c_r\right)^{\beta_r}$$

unde: $k \in \mathbb{N}$, $a_1, \ldots, a_k$ sînt reale, distincte două cîte două şi $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$; $r \in \mathbb{N}$, $X^2 + b_i X + c_i$, $1 \leq i \leq r$, sînt polinoame ireductibile ($b_i^2 - 4a_i c_i < 0$) şi distincte două cîte două, iar $\beta_1, \ldots, \beta_r \in \mathbb{N}$.

Atunci funcţia raţională P/Q se scrie în mod unic sub forma:

$$\frac{P}{Q} = L + \sum_{i=1}^{k} \left(\frac{d_{i,1}}{(X - a_i)} + \ldots + \frac{d_{i,\alpha_i}}{(X - a_i)^{\alpha_i}} \right) + \sum_{j=1}^{r} \left(\frac{e_{j,1} X + f_{j,1}}{\left(X^2 + b_j X + c_j\right)} + \ldots + \frac{e_{j,\beta_j} X + f_{j,\beta_j}}{\left(X^2 + b_j X + c_j\right)^{\beta_j}} \right)$$

unde: $L \in \mathbb{R}[X]$, $d_{i,t} \in \mathbb{R}$, $(1 \leq i \leq k, 1 \leq t \leq \alpha_k)$, $e_{j,s}, f_{j,s} \in \mathbb{R}$, $(1 \leq j \leq r, 1 \leq s \leq \beta_r)$.

Demonstraţie. Vezi exerciţiile. □

Propoziţia următoare dă cîteva criterii generale de ireductibilitate.

3.18 Propoziție. *Fie R un inel integru, K corpul său de fracții și* $f = a_0 + a_1X + \dots + a_nX^n$ *un polinom nenul cu coeficienți în R* ($n \ge 2$).

a) Fie c, d $\in R$, *cu c inversabil în R. Atunci f este ireductibil dacă și numai dacă* $f(cX + d)$ *este ireductibil.*

b) Presupunem că $a_0 \ne 0$. *Atunci f este ireductibil dacă și numai dacă polinomul*

$$r(f) = a_n + a_{n-1}X + \dots + a_0X^n,$$

numit „polinomul reciproc al lui f" este ireductibil.

c) Presupunem că f nu are divizori neinversabili de grad 0. *Dacă S este un inel comutativ și* $\varphi : R \to S$ *este un morfism de inele astfel încît* $\varphi(a_n) \ne 0$ *și polinomul* $\varphi(a_0) + \varphi(a_1)X + \dots + \varphi(a_n)X^n$ *este ireductibil în* $S[X]$, *atunci f este ireductibil în* $R[X]$.

d) (Criteriul lui Eisenstein) *Fie R un inel factorial. Dacă există un element prim* $p \in R$ *astfel încît* $p | a_i$, $\forall\ i < n$, $p \nmid a_n$, $p^2 \nmid a_0$, *atunci f este ireductibil în* $K[X]$ (*deci f ireductibil și în* $R[X]$ *dacă este primitiv*).

Demonstrație. *a)* Fie $\varphi : R[X] \to R[X]$ unicul morfism de R-algebre cu proprietatea că $\varphi(X) = cX + d$. Altfel spus, $\varphi(f)$ se obține înlocuind nedeterminata X în polinomul f cu $cX + d$. Elementul c este inversabil dacă și numai dacă φ este izomorfism de R-algebre (morfismul de R-algebre $\psi : R[X] \to R[X]$ care duce X în $c^{-1}X - c^{-1}d$ este inversul lui φ). Avem așadar $f = gh \Leftrightarrow \varphi(f) = \varphi(g)\varphi(h)$, $\forall g, h \in R[X]$. Observînd că φ păstrează gradele și că $\varphi|_R = \mathrm{id}_R$, se obține imediat că f este ireductibil dacă și numai dacă $\varphi(f)$ este ireductibil.

b) Dacă g și h sînt polinoame din $R[X]$, cu termenul liber nenul, atunci $r(gh) = r(g)r(h)$. Într-adevăr, observăm că $r(f) = X^n f\left(\frac{1}{X}\right)$ (pentru rigurozitatea argumentului se consideră egalitățile în $K(X)$, corpul de fracții al lui $K[X]$). Deci, dacă grad $g = m$, grad $h = p$, avem

$$r(gh) = X^{m+p}(gh)\left(\frac{1}{X}\right) = X^m g\left(\frac{1}{X}\right) X^p h\left(\frac{1}{X}\right) = r(g)r(h).$$

Concluzia rezultă observînd că r păstrează gradele și că, pentru orice $d \in R$, avem $d | f \Leftrightarrow d | r(f)$.

c) Fie $\psi : R[X] \to S[X]$ unicul morfism de R-algebre (adică ψ este morfism de inele și $\psi|_R = \varphi$) astfel încît $\psi(X) = X$. Avem de demonstrat că $\psi(f)$ ireductibil implică f ireductibil. Presupunem că $f = gh$, cu $g, h \in R[X]$. Atunci $\psi(f) = \psi(g)\psi(h)$; condiția $\varphi(a_n) \ne 0$ asigură că $\mathrm{grad}\,\psi(g) + \mathrm{grad}\,\psi(h) = \mathrm{grad}\,\psi(f) = n$. Cum $\mathrm{grad}\,\psi(q) \le \mathrm{grad}\, q$, $\forall q \in R[X]$, obținem că $\mathrm{grad}\,\psi(g) = \mathrm{grad}\, g$ și $\mathrm{grad}\,\psi(h) = \mathrm{grad}\, h$. Din ireductibilitatea lui $\psi(f)$ deducem că $\psi(g)$ (pentru a face o alegere) este inversabil, deci are grad 0. Astfel, $0 = \mathrm{grad}\,\psi(g) = \mathrm{grad}\, g$. Cum f nu are divizori neinversabili de grad 0, $g \in U(R)$.

d) Scriind $f = c(f)\cdot f'$, cu f' primitiv, avem că f și f' sînt asociate în $K[X]$. Înlocuind polinomul f cu f', putem presupune că f este primitiv. Este suficient acum să demonstrăm că f este ireductibil în $R[X]$. Dacă f ar fi reductibil, atunci:

$$f = a_0 + a_1X + \dots + a_nX^n = (b_0 + b_1X + \dots + b_mX^m)\,(c_0 + c_1X + \dots + c_pX^p),$$

unde $m > 0$, $p > 0$, $b_0, b_1, \ldots, b_m, c_0, c_1, \ldots, c_p \in R$, $b_m \neq 0$, $c_p \neq 0$. Avem $b_0c_0 = a_0$, deci $p \mid b_0c_0$ şi $p^2 \nmid b_0c_0$; de aici rezultă că p divide exact unul din elementele b_0 şi c_0. Presupunem că $p \mid b_0$ şi $p \nmid c_0$. Întrucît $p \nmid a_n$, p nu divide toţi coeficienţii b_i; există aşadar un i minim, $1 \leq i \leq m$, astfel încît $p \nmid b_i$ (şi deci $p \mid b_j$, $\forall j < i$). Atunci $p \nmid b_ic_0$ şi deci elementul

$$a_i = b_ic_0 + \sum_{j=1}^{i-1} b_j c_{i-j}$$

nu se divide cu p, contradicţie cu ipoteza. □

Există *algoritmi* de decizie a ireductibilităţii pentru polinoame din $\mathbb{Z}[X]$ (deci şi pentru cele din $\mathbb{Q}[X]$), un asemenea algoritm (datorat lui Kronecker) fiind descris în exerciţiul **19.** O aplicare repetată a unui astfel de algoritm conduce la un *algoritm de factorizare* (de descompunere în factori ireductibili) a oricărui polinom din $\mathbb{Q}[X]$. Programele moderne de calcul simbolic (*Maple, Mathematica, Macaulay, Axiom,* etc.) au implementate rutine puternice de decizie a ireductibilităţii, inclusiv pentru polinoame de mai multe variabile şi pentru polinoame cu coeficienţi în extinderi algebrice ale lui $\mathbb{Q}$ sau într-un corp finit. Se poate demonstra că, dacă există un algoritm de factorizare pentru $K[X]$, cu K un corp, atunci există unul şi pentru $L[X]$, oricare ar fi L o extindere finit generată a lui K. În particular, există algoritm de factorizare pentru $K[X_1,\ldots, X_n]$. Pentru detalii şi dezvoltări recente, vezi de ex. ALBU şi ION [1997], SPINDLER [1994], GEDDES, CZAPOR, LABAHN [1992], WINKLER [1996].

3.19 Exemple. a) Polinomul $6X^9 + 13X^2 + 26$ este ireductibil în $\mathbb{Q}[X]$ (şi în $\mathbb{Z}[X]$, căci este primitiv), conform criteriului lui Eisenstein aplicat cu $p = 13$.

b) Pentru orice număr prim p şi orice $n \in \mathbb{N}^*$, $X^n - p$ este ireductibil în $\mathbb{Q}[X]$ şi în $\mathbb{Z}[X]$ (tot cu criteriul lui Eisenstein).

c) Fie p un număr prim şi $f = X^{p-1} + X^{p-2} + \ldots + X + 1 \in \mathbb{Z}[X]$. Criteriul lui Eisenstein nu este aplicabil direct lui f. Considerînd însă polinomul

$$g = f(X+1) = \frac{(X+1)^p - 1}{X+1-1} = \sum_{i=1}^{p} C_p^i X^{i-1} ,$$

observăm că lui g i se poate aplica criteriul lui Eisenstein, căci p divide toţi coeficienţii binomiali C_p^i cu $1 \leq i < p$. Deci g este ireductibil şi astfel, conform punctului *a)* al propoziţiei de mai sus, f este ireductibil.

d) Polinomul $f = Y^9 + X^9Y^7 - 3X^2Y + 2X$ este ireductibil în $\mathbb{Z}[X, Y]$. Pentru demonstraţie, considerăm f ca polinom în Y cu coeficienţi în inelul factorial $\mathbb{Z}[X]$. Aplicăm acum criteriul lui Eisenstein cu $p = X$ (X este element ireductibil în $\mathbb{Z}[X]$). Remarcăm că inelul $\mathbb{Z}$ putea fi înlocuit cu orice inel factorial de caracteristică diferită de 2.

e) Considerăm polinomul $f = X^5 + X^2 + 1 \in \mathbb{Z}_2[X]$. Polinomul f nu are rădăcini în $\mathbb{Z}_2$, deci divizorii proprii ai lui f nu pot fi de grad 1 (sînt de grad 2 sau 3). O descompunere a lui f poate fi doar de forma:

$$X^5 + X^2 + 1 = (X^3 + aX^2 + bX + 1)(X^2 + cX + 1),$$

cu $a, b, c \in \mathbb{Z}_2$. Identificînd coeficienții, se obține un sistem de ecuații în a, b, c, despre care se vede imediat că nu are soluții în $\mathbb{Z}_2$. Aşadar, f este ireductibil în $\mathbb{Z}_2[X]$.

f) O aplicare tipică a criteriului 3.18.*c)* la un polinom f cu coeficienți întregi constă în a „reduce coeficienții modulo n". Mai precis, pentru un $n \in \mathbb{N}$ convenabil ales, se consideră unicul morfism de inele $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ şi se cercetează ireductibilitatea polinomului „f redus modulo n" (notat cu $\psi(f)$ în demonstrație). Fie, de exemplu, polinomul $f = 7X^5 + 4X^3 - X^2 + 6X + 9 \in \mathbb{Z}[X]$. Redusul modulo 2 al lui f este $X^5 + X^2 + 1 \in \mathbb{Z}_2[X]$, despre care am văzut că este ireductibil. Condițiile de la 3.18.*c)* sînt îndeplinite, deci f este ireductibil în $\mathbb{Z}[X]$ (deci şi în $\mathbb{Q}[X]$, fiind primitiv).

g) Polinomul $10X^7 + 5X^2 + 2$ este ireductibil în $\mathbb{Z}[X]$, căci reciprocul său este $2X^7 + 5X^5 + 10$, căruia i se poate aplica criteriul lui Eisenstein cu $p = 5$.

Exerciții

În exerciții, R este un inel integru şi K este corpul său de fracții (dacă nu se specifică altfel).

1. Orice inel integru finit este corp.

2. Fie R un inel unitar infinit. Demonstrați că mulțimea $R°$ a elementelor nenule şi neinversabile este infinită. (Ind. Dacă $R°$ este finită, atunci $U(R)$ este infinită. Fie $S(R°)$ mulțimea bijecțiilor de la $R°$ la $R°$. Aplicația $\varphi : U(R) \to S(R°)$ $x \mapsto \varphi_x$, $\varphi_x(a) = xa$, $\forall a \in R°$, este injectivă, contradicție.)

3. Fie R un inel integru în care orice două elemente au cmmdc. Atunci orice element din K se poate scrie sub forma a/b, $(b \neq 0)$, cu $a, b \in R$, prime între ele („fracția a/b este ireductibilă"). Ce se poate spune despre unicitatea unei astfel de scrieri?

4. Arătați că un inel comutativ R este integru dacă şi numai dacă $R[X]$ este integru.

5. Fie $p \in R°$. Demonstrați că idealul generat de p în $R[X]$, $pR[X]$, este prim dacă şi numai dacă p este element prim în R. (Ind.: Arătați că $R[X]/(pR[X]) \cong (R/pR)[X]$). Deduceți o nouă demonstrație pentru 2.19.*a)*.

6. Fie $d \in \mathbb{Z}$, liber de pătrate (adică d nu se divide cu pătratul nici unui întreg > 1), şi $\mathbb{Z}[\sqrt{d}\,] := \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$. Definim „*norma*" $\mathrm{N} : \mathbb{Z}[\sqrt{d}\,] \to \mathbb{Z}$, $\mathrm{N}(a + b\sqrt{d}) = a^2 - db^2$, $\forall\, a, b \in \mathbb{Z}$. Atunci:

a) $\mathrm{N}(\alpha)\mathrm{N}(\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$, $\forall \alpha, \beta \in \mathbb{Z}[\sqrt{d}\,]$.

b) $U(\mathbb{Z}[\sqrt{d}\,]) = \{\alpha \in \mathbb{Z}[\sqrt{d}\,] \mid \mathrm{N}(\alpha) = \pm 1\} = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}, a^2 - db^2 = \pm 1\}$.

Determinați efectiv $U(\mathbb{Z}[\sqrt{d}\,])$ dacă $d < 0$.

7. Elementele 6 şi $2 + \sqrt{-5}$ nu au cmmdc (şi deci nici cmmmc) în inelul $\mathbb{Z}[\sqrt{-5}\,]$.

8. Un număr prim $p \in \mathbb{Z}$ este prim şi în inelul $\mathbb{Z}[i]$ dacă şi numai dacă $4 \mid p - 1$.

9. Fie R un inel euclidian faţă de funcţia φ. Atunci există $u \in R$ nenul şi neinversabil cu proprietatea: $\forall x \in R$, $\exists q \in R$ astfel încît $x - qu$ este inversabil sau 0. Cîtpoate fi ales u pentru $R = \mathbb{Z}$, $K[X]$? (*Ind.* min $\{\varphi(v) \mid v \in R°\} = \varphi(u)$ pentru un $u \in R°$.)

10. Fie d un întreg liber de pătrate, $d \equiv 1 \pmod 4$. Atunci inelul $\mathbb{Z}[\sqrt{d}\,]$ nu este GCD-inel. (*Ind.* 2 este ireductibil şi nu este prim.)

11. Să se arate că în $\mathbb{Z}$ există o infinitate de elemente prime neasociate în divizibilitate.

12. Fie R un inel principal, $n \in \mathbb{N}^*$, $a_1, \dots, a_n \in R$ şi d un cmmdc al lor. Demonstraţi că există $u_1, \dots, u_n \in R$ astfel încît $d = a_1u_1 + \dots + a_nu_n$.

13. Fie R un inel factorial şi $f = a_0 + a_1X + \dots + a_nX^n \in R[X]$.

a) Dacă $p/q \in K$ este o rădăcină a lui f, unde $p, q \in R$ şi $(p, q) = 1$, atunci $p|a_0$, $q|a_n$ şi $(p - qr)|f(r)$, $\forall r \in R$. Ce devin relaţiile pentru $a_n = 1$?

b) Fie $g = a_n^{n-1}a_0 + a_n^{n-2}a_1X + \dots + a_{n-1}X^{n-1} + X^n$. Atunci $a_n^{n-1}f(X) = g(a_nX)$. Descrieţi legătura dintre rădăcinile lui g şi cele ale lui f.

c) Găsiţi rădăcinile din $\mathbb{Q}$ ale polinoamelor $2X^3 + 5X^2 + 9X - 15$ şi $4X^3 - 7X^2 - 7X + 15$.

14. Fie K un corp. Demonstraţi că orice polinom nenul $f \in K[X]$ are cel mult grad f rădăcini în K (fiecare fiind numărată cu multiplicitatea sa).

15. Fie R un inel. Demonstraţi echivalenţa următoarelor afirmaţii:

a) Orice polinom nenul $f \in R[X]$ are cel mult grad f rădăcini în R (fiecare fiind numărată cu multiplicitatea sa).

b) Orice polinom de grad 1 are cel mult o rădăcină în R.

c) R este inel integru.

(Ind. Consideraţi corpul de fracţii al lui R şi folosiţi problema precedentă).

16. Fie K un corp. Vrem să demonstrăm, într-un caz mai general, teorema de descompunere a unei funcţii raţionale în sumă de funcţii raţionale simple.

a) Fie $Q \in K[X]$, ireductibil. Atunci, pentru orice $k \in \mathbb{N}$ şi $P \in K[X]$, există o scriere de forma:

$$\frac{P}{Q} = L + \frac{f_1}{Q} + \dots + \frac{f_k}{Q^k},$$

unde $L, f_1, \dots, f_k \in K[X]$ şi grad $f_i <$ grad Q. (*Ind*. Cazul $k = 1$ se reduce la teorema împărţirii cu rest a lui P la Q. În continuare se aplică o inducţie după k.)

b) Fie $Q \in K[X]$, $Q = q_1^{\alpha_1} \dots q_k^{\alpha_k}$, cu q_i ireductibile în $K[X]$, prime între ele două cîte două. Atunci, pentru orice $P \in K[X]$, există o scriere de forma:

$$\frac{P}{Q} = L + \sum_{i=1}^{k}\left(\frac{f_{i,1}}{q_i} + \dots + \frac{f_{i,\alpha_i}}{q_i^{\alpha_i}}\right),$$

unde $L, f_{i,t} \in K[X]$ şi grad $f_{i,t} <$ grad q_i, pentru orice i şi t.

(*Ind.* Fie $u_i = \dfrac{Q}{q_i^{\alpha_i}} \in K[X]$. Avem $(u_1, \ldots, u_n) = 1$, deci există $v_1, \ldots, v_n \in K[X]$ astfel încît $u_1v_1 + \ldots + u_nv_n = 1 \Rightarrow P = Pu_1v_1 + \ldots + Pu_nv_n \Rightarrow \dfrac{P}{Q} = \dfrac{Pv_1}{q_1^{\alpha_1}} + \ldots + \dfrac{Pv_k}{q_k^{\alpha_k}}$. Se aplică acum a) pentru fiecare termen.)

c) (unicitatea scrierii) Dacă $L + \sum_{i=1}^{k}\left(\dfrac{f_{i,1}}{q_i} + \ldots + \dfrac{f_{i,\alpha_i}}{q_i^{\alpha_i}}\right) = M + \sum_{i=1}^{k}\left(\dfrac{g_{i,1}}{q_i} + \ldots + \dfrac{g_{i,\alpha_i}}{q_i^{\alpha_i}}\right)$, unde $L, M, f_{i,t}, g_{i,t} \in K[X]$ şi grad $f_{i,t}$, grad $g_{i,t} <$ grad q_i, pentru orice i şi t, atunci $L = R$ şi $f_{i,t} = g_{i,t}$, $\forall i, t$. (*Ind.* Înmulţind cu Q, se obţine o relaţie de forma $LQ + R_1 = MQ + R_2$, unde grad R_1 şi grad R_1 sînt < grad Q. Din unicitatea împărţirii cu rest la Q rezultă că $L = M$ şi $R_1 = R_2$. Rămîne de demonstrat că, dacă $\sum_{i=1}^{k}\left(\dfrac{f_{i,1}Q}{q_i} + \ldots + \dfrac{f_{i,\alpha_i}Q}{q_i^{\alpha_i}}\right) = 0$ şi grad $f_{i,t} <$ grad q_i, atunci $f_{ij} = 0$, $\forall i, j$. Pentru i fixat, se observă că q_i apare ca factor pentru toţi termenii din membrul stîng, cu excepţia lui $\dfrac{f_{i,\alpha_i}Q}{q_i^{\alpha_i}}$. Cum q_i este prim cu $\dfrac{Q}{q_i^{\alpha_i}}$, rezultă că $q_i \mid f_{i,\alpha_i}$, deci $f_{i,\alpha_i} = 0$ din motive de grade. Se împarte acum relaţia la q_i şi se repetă raţionamentul, obţinîndu-se $f_{i,\alpha_i - 1} = 0$ etc.)

d) Demonstraţi teorema IV.3.17, punînd $K = \mathbb{R}$.

17. Fie R un inel. Dacă $f \in R[X]$, i se asociază *funcţia polinomială* $\widetilde{f} : R \to R$ unde, $\forall x \in R$, $\widetilde{f}(x) = f(x)$ (valoarea polinomului f în x). Demonstraţi că, dacă R este integru infinit, atunci funcţia $\varphi : R[X] \to R^R$, $\varphi(f) = \widetilde{f}$, $\forall f \in R[X]$, este injectivă. Rămîne valabilă concluzia dacă se renunţă la ipoteza R infinit?

18. (*Polinomul de interpolare Lagrange*) Fie K un corp, $n \geq 1$, $x_0, \ldots, x_n \in K$, ($n + 1$ elemente distincte) şi $y_0, \ldots, y_n \in K$. Demonstraţi că există un unic polinom $L \in K[X]$ de grad cel mult n astfel încît $L(x_i) = y_i$, $0 \leq i \leq n$.

19. (Algoritmul de factorizare al lui Kronecker în $\mathbb{Z}[X]$) Fie $p \in \mathbb{Z}[X]$, primitiv, grad $p = n$. Notăm cu m cel mai mare întreg $\leq n/2$.

a) Arătaţi că p reductibil în $\mathbb{Z}[X] \Leftrightarrow p$ are un factor neconstant de grad $\leq m$.

b) Fie $(x_0, \ldots, x_m) \in \mathbb{Z}^{m+1}$, cu x_i distincte două cîte două. Arătaţi că următorul algoritm se termină într-un număr finit de paşi şi furnizează un factor neconstant al lui p de grad $\leq m$ sau demonstrează ireductibilitatea lui p:

1. Dacă $\exists i$ cu $p(x_i) = 0$, atunci $X - x_i$ este un factor al lui p şi am terminat. Dacă nu, treci la *2.*

2. Fie $D = \{d = (d_0, \ldots, d_m) \in \mathbb{Z}^{m+1} \mid d_i \mid p(x_i), \forall i\}$. D este o mulţime finită. Pentru orice $d \in D$, fie $L_d \in \mathbb{Q}[X]$ polinomul (de interpolare Lagrange) cu proprietăţile $L_d(x_i) = d_i$, $\forall i$, şi grad $L_d \leq m$. Dacă există $d \in D$ cu $L_d \in \mathbb{Z}[X]$ şi $L_d \mid p$, atunci L_d este un factor al lui p şi am terminat. Dacă nu, atunci *p este ireductibil*.

c) Deduceţi un algoritm de decizie a ireductibilităţii pentru polinoame din $\mathbb{Q}[X]$.

d) Presupunem că $m = 2$. Ce alegere pentru $(x_0, \ldots, x_m)$ propuneți?

e) Presupunem că în inelul factorial R există un algoritm de factorizare (de descompunere a oricărui element din $R°$ în factori primi). Ce proprietăți trebuie să aibă R pentru a putea generaliza la $R[X]$ algoritmul de mai sus?

f) Presupunem că R este factorial şi că în $R[X]$ există un algoritm de factorizare. Atunci există un algoritm de factorizare în $K[X]$.

20. Decideți ireductibilitatea polinomului $X^4 + X^2 + 2X - 1$ din $\mathbb{Z}[X]$ cu algoritmul Kronecker.

21. Fie R un inel integru.

a) Fie $f \in R[X]$, grad $f = m$. Dacă f are cel puțin $m + 1$ rădăcini în R, atunci $f = 0$.

b) Fie $g \in R[X_1,\ldots, X_n]$, cu R *infinit*. Dacă $g(a_1, \ldots, a_n) = 0$, $\forall (a_1, \ldots, a_n) \in R^n$, atunci g este polinomul nul. (*Ind*. Inducție după n.) Deduceți că două polinoame din $R[X_1,\ldots, X_n]$ sînt egale dacă şi numai dacă funcțiile polinomiale asociate sînt egale.

c) Dați exemplu de corp finit K şi de polinoame distincte din $K[X]$ care au aceeaşi funcție polinomială asociată.

22. Fie K un corp de caracteristică diferită de 2 (adică $1 + 1 \neq 0$ în K) şi p un polinom omogen de grad 2 în $K[X, Y]$, adică $p = aX^2 + bXY + cY^2$, cu $a, b, c \in K$. Demonstrați că p este reductibil în $K[X, Y] \Leftrightarrow b^2 - 4ac$ este un pătrat în $K \Leftrightarrow b^2 - 4ac = 0$ sau există $\alpha, \beta \in K$, $(\alpha, \beta) \neq (0, 0)$, cu $p(\alpha, \beta) = 0$.

23. Să se descompună în factori ireductibili polinomul $X_1^3 + X_2^3 \in K[X_1, X_2]$. Discuție după caracteristica lui K.

24. Fie K un corp de caracteristică diferită de 3 şi $f = X_1^3 + \ldots + X_n^3 \in K[X_1,\ldots, X_n]$. Arătați că f este ireductibil dacă şi numai dacă $n \geq 3$. Generalizare. (*Ind.* Pentru $n = 3$, folosiți criteriul Eisenstein pentru $f \in K[X_1, X_2][X_3]$. Se face apoi o inducție după n.)

25. Fie n^2 nedeterminate X_{ij}, $1 \leq i, j \leq n$ şi matricea $A = (X_{ij})_{1 \leq i, j \leq n} \in \mathrm{M}_n(\mathbb{Z}[X_{ij}; 1 \leq i, j \leq n])$. Atunci polinomul $\det A = \sum\{X_{1\sigma(1)^{\nu}} \ldots X_{n\sigma(n)} \mid \sigma \in S_n\}$ este ireductibil în $\mathbb{Z}[X_{ij}; 1 \leq i, j \leq n]$.

26. Fie $x, y \in R$. Dacă există un cmmmc al lor $[x, y] \in R$, atunci există şi un cmmdc al lor (x, y) şi avem $xy \sim [x, y](x, y)$.

27. Fie R un subinel unitar al unui inel comutativ S. Un element al lui S se numeşte *întreg* peste R dacă este rădăcină a unui polinom unitar nenul din $R[X]$. Demonstrați că, dacă R este GCD-inel şi $x \in K$ este întreg peste R, atunci $x \in R$.

28. Fie R un inel principal şi S un sistem multiplicativ închis în R. Atunci inelul de fracții $S^{-1}R$ este principal.

29. Fie R un inel factorial şi S un sistem multiplicativ închis în R. Atunci inelul de fracții $S^{-1}R$ este factorial.

30. Proprietatea unui inel R de a fi euclidian (respectiv principal, factorial) se transmite şi la subinelele unitare ale lui R?

31. Fie R un inel factorial care nu este corp, astfel încît grupul unităților $U(R)$ este finit. Atunci în R există o infinitate de elemente prime neasociate în divizibilitate. (*Ind.* Dacă $p_1, \ldots, p_n$ sînt toate elementele prime pînă la asociere, atunci există $m \geq 1$ astfel încît $1 + (p_1 \ldots p_n)^m \in R°$.)

32. Fie R un inel factorial și $p \in R$ un element prim. Folosind morfismul canonic $\pi : R \to R/pR$ și prelungirea sa la un morfism $\psi : R[X] \to (R/pR)[X]$, dați o nouă demonstrație criteriului lui Eisenstein. (Ind. Dacă $f = a_0 + a_1 X + \ldots + a_n X^n$ satisface ipotezele criteriului și $f = gh$, atunci $\psi(f) = \pi(a_n)X^n = \psi(g)\psi(h)$. Dacă grad g, grad $h \geq 1$, atunci termenii liberi ai lui g și h sînt multipli de p.)

V. Spații liniare, matrice şi aplicații

V.1 Algebre de matrice

Scopul acestei secțiuni este de a da demonstrații scurte şi relativ elementare teoremelor Cayley-Hamilton şi Frobenius folosind polinoamele matriciale.

1.1 Definiție. O matrice $m\times n$ cu elemente polinoame din $K[X]$ se numeşte *polinom matricial* peste corpul K. Putem scrie un polinom matricial $P \in \mathrm{M}(m, n, K[X])$ sub forma:

$$P = \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & & \\ p_{n1} & \cdots & p_{nn} \end{bmatrix}, \text{ cu } p_{ij} \in K[X], \tag{1}$$

sau (grupînd după puterile lui X) sub forma:

$$P = P_0 + X P_1 + \ldots + X^r P_r, \tag{2}$$

unde $P_0, P_1, \ldots, P_r \in \mathrm{M}(m, n, K)$.

De exemplu, avem:

$$\begin{bmatrix} 5+2X & 3X^3 \\ 1 & 2-2X+X^2 \end{bmatrix} = \begin{bmatrix} 5 & 0 \\ 1 & 2 \end{bmatrix} + X\begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix} + X^2\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} + X^3\begin{bmatrix} 0 & 3 \\ 0 & 0 \end{bmatrix}$$

1.2 Definiție. Fie $P \in \mathrm{M}(n, K[X])$ un polinom matricial de forma (2), cu P_i matrice *pătratice* ($\in \mathrm{M}(n, K)$), iar $A \in \mathrm{M}(n, K)$. Definim $P(A)$, *valoarea lui P în A:*

$$P(A) := P_0 + AP_1 + \ldots + A^r P_r \in \mathrm{M}(n, K).$$

1.3 Observație. Dacă P, $Q \in \mathrm{M}(n, K[X])$ sînt polinoame matriciale, atunci avem definite $P+Q$, PQ (operațiile uzuale în $\mathrm{M}(n, K[X])$). Pentru $\forall A \in \mathrm{M}(n, K)$, au sens $(P+Q)(A)$ şi $(PQ)(A)$, definite ca mai sus. Are loc $(P+Q)(A) = P(A) + Q(A)$ (demonstrație uşoară), *însă în general* $(PQ)(A) \neq P(A)Q(A)$. De exemplu, dacă P şi Q sînt "de grad 1", $P = XP_1$ şi $Q = XQ_1$, cu P_1, $Q_1 \in \mathrm{M}(n, K)$, atunci $PQ = X^2P_1Q_1$. Avem $P(A)Q(A) = AP_1AQ_1$, $(PQ)(A) = A^2P_1Q_1$ şi $AP_1AQ_1 \neq A^2P_1Q_1$ în general. Totuşi, are loc:

1.4 Propoziție. *Dacă* $P = P_0 + X P_1 + \ldots + X^r P_r$ *şi* $AP_i = P_i A$, $1 \le i \le r$ (*A comută cu* P_i, $\forall i$), *atunci* $(PQ)(A) = P(A)Q(A)$, $\forall Q = Q_0 + X Q_1 + \ldots + X^d Q_d \in \mathrm{M}(n, K[X])$.

Demonstrație. PQ se obține prin regula uzuală (atenție la ordinea factorilor!):

$$PQ = P_0Q_0 + X(P_0Q_1 + P_1Q_0) + \ldots + X^{r+d}P_rQ_d,$$

$$\text{iar } P(A)Q(A) = (P_0 + AP_1 + \ldots + A^rP_r)(Q_0 + AQ_1 + \ldots + A^dQ_d).$$

Un termen oarecare al produsului $P(A)Q(A)$ este de forma $A^iP_i A^jQ_j = A^iA^jP_iQ_j = A^{i+j}P_iQ_j$ (căci P_i comută cu A^j).Grupînd termenii ce conțin A^k ($0 \le k \le r + d$), rezultă că

$$P(A)Q(A) = P_0Q_0 + A(P_0Q_1 + P_1Q_0) + \ldots + A^{r+d}P_rQ_d = (PQ)(A).$$

1.5 Teoremă.(Teorema Cayley-Hamilton[72]) *Fie K un corp,* $A \in \mathrm{M}(n, K)$ *şi* $f_A = \det(XI - A)$ *polinomul său caracteristic. Atunci* $f_A(A) = 0$.

Demonstrație. Se ştie că, dacă $B = (b_{ij}) \in \mathrm{M}(n, R)$ este o matrice cu coeficienți într-un inel comutativ R, are loc: $B\cdot\mathrm{ad}(B) = \det(B)\cdot I$, unde este $\mathrm{ad}(B)$ matricea reciprocă (adjunctă) a lui B (pe locul (i, j) al lui $\mathrm{ad}(B)$ este complementul algebric al lui b_{ij} în B). Aplicînd această observație matricei $XI - A \in \mathrm{M}(n, K[X])$, are loc

$$(XI - A)\cdot\mathrm{ad}(XI - A) = \begin{bmatrix} \det(XI-A) & & 0 \\ & \ddots & \\ 0 & & \det(XI-A) \end{bmatrix} =: P,$$

Din lema următoare rezultă $P(A) = 0$, iar $P(A) = f_A(A)$, deci $f_A(A) = 0$. □

1.6 Lemă. *Fie* $P \in \mathrm{M}(n, K[X])$ *un polinom matricial şi* $A \in \mathrm{M}(n, K)$. *Atunci* $P(A) = 0 \Leftrightarrow$ *există* $Q \in \mathrm{M}(n, K[X])$ *astfel încît* $P = (XI - A)\cdot Q$.

Demonstrație. Fie $P = P_0 + X P_1 + \ldots + X^rP_r$. Avem:

$P - P(A) = P_0 + X P_1 + \ldots + X^rP_r - (P_0 + A P_1 + \ldots + A^rP_r) =$

$(XI - A)P_1 + (X^2I - A^2)P_2 + \ldots + (X^rI - A^r)P_r$.

Însă $X^kI - A^k = (XI - A)(X^{k-1}I + X^{k-2}A + \ldots + A^{k-1})$, $\forall k$. Înlocuind în relația de mai sus, avem $P - P(A) = (XI - A)Q$, cu $Q \in \mathrm{M}(n, K[X])$. Dacă $P(A) = 0$, rezultă $P = (XI - A)Q$.

Reciproc, fie $P = (XI - A)Q$. Cum coeficienții lui $XI - A$ sînt I şi $A \in \mathrm{M}(n, K)$ (care comută cu A), din observația **1.4** rezultă că $P(A) = (AI - A)Q(A) = 0$. □

Pentru o matrice dată $A \in M(n, K)$, polinomul caracteristic f_A nu este neapărat de grad minim printre polinoamele $p \in K[X]$ cu $p(A) = 0$.

1.7 Propoziție. *Fie* $A \in M(n, K)$. *Există un unic polinom unitar* $\mu_A \in K[X]$ *cu proprietățile*:

a) $\mu_A(A) = 0$;

b) $\forall p \in K[X]$ *cu* $p(A) = 0$ *rezultă că* $\mu_A \mid p$.

În plus, μ_A *este polinomul unitar de grad minim printre polinoamele* $p \in K[X]$ *cu* $p(A) = 0$.

---

[72] Arthur Cayley (1821-1895) şi Sir William Rowan Hamilton (1805-1865), matematicieni britanici. Cazul general al teoremei a fost demonstrat însă de Frobenius.

Demonstrație. Fie $M = \{p \in K[X] \mid p \neq 0, p(A) = 0\}$. M este nevidă ($f_A \in M$). Mulțimea de numere naturale $\{\text{grad}\, p \mid p \in M\}$ are un cel mai mic element, deci există $\mu_A \in M$ (îl putem alege unitar) astfel încît $\text{grad}\mu_A \leq \text{grad}\, p$, $\forall p \in M$. Fie $p \in M$. Atunci există $q, r \in K[X]$ astfel încît $p = \mu_A q + r$, cu $\text{grad}\, r < \text{grad}\mu_A$. Avem $0 = p(A) = \mu_A(A)q(A) + r(A) = r(A)$, deci $r = 0$ (dacă $r \neq 0$, ar rezulta $r \in M$ şi $\text{grad}\, r < \text{grad}\mu_A$, contradicție cu alegerea lui μ_A). Astfel, $\mu_A \mid p$. Dacă $q \in K[X]$ este unitar şi satisface condițiile *a)* şi *b)*, atunci $\mu_A \mid q$ şi $q \mid \mu_a$. Cum μ_A este unitar, rezultă $\mu_A = q$. □

1.8 Definiție. Fie $A \in M(n, K)$. Polinomul unitar $\mu_A \in K[X]$ din propoziția precedentă se numeşte *polinomul minimal* al lui A.

1.9 Teoremă. *Fie $A \in M(n, K)$. Atunci:*

a) Polinomul minimal μ_A divide polinomul caracteristic f_A.

b) (Frobenius[73]) *Polinomul minimal μ_A şi polinomul caracteristic f_A au aceleaşi rădăcini*[74] *(posibil cu multiplicități diferite).*

Demonstrație. *a)* Clar, din definiția lui μ_A.

b) Dacă $f_A(\lambda) = 0$, atunci λ este valoare proprie a lui A, deci $Ax = \lambda x$ pentru un $x \in E$, nenul. Rezultă că $A^r x = \lambda^r x$, $\forall r \in \mathbb{N}$ şi, mai general, $p(A)\cdot x = p(\lambda)x$, $\forall p \in K[X]$. Deci $0 = \mu_A(A)\cdot x = \mu_A(\lambda)\cdot x$, de unde $\mu_A(\lambda) = 0$. Invers, orice rădăcină a lui μ_A este rădăcină a lui f_A, căci $\mu_A \mid f_A$. □

V.2 Coduri liniare corectoare de erori

Algebra liniară îşi găseşte un domeniu fertil şi neaşteptat de aplicabilitate în teoria *codurilor corectoare de erori*, teorie născută în anii 1940, odată cu era calculatoarelor şi a comunicațiilor digitale. Vom prezenta ideile de bază din această teorie şi cîteva aplicații ale algebrei liniare, relativ elementare, dar cu utilitate practică deosebită.

Prin "informație digitală" înțelegem un şir de simboluri (elemente) dintr-un alfabet finit. De exemplu, 011110101100 este un şir de simboluri din alfabetul {0,1} (în acest caz, simbolurile se numesc *biți*). Transmiterea unei *informații digitale*[75] între două puncte diferite *în spațiu* (de exemplu o transmisie de date pe o linie telefonică) sau *în timp* (stocarea pe un

---

[73] Ferdinand Georg Frobenius (1849-1917), matematician german.

[74] Este vorba de rădăcinile din K. Enunțul rămîne valabil şi pentru rădăcinile dintr-o *extindere* L a lui K (un corp L astfel încît K este subcorp în L).

[75] Transmiterea de sunete, imagini, texte etc. ca un şir de 0 şi 1 pare azi evidentă, dar în anii 1940 a fost o idee revoluționară şi îi aparține lui *Claude Shannon* (1916-2001), matematician american, unul din fondatorii teoriei informației (articolul *A mathematical theory of communication,* 1948).

suport material cum ar fi un compact disc, pentru o citire ulterioară), este supusă *erorilor* cauzate de o varietate de factori: zgomot pe linia telefonică, deteriorarea suportului fizic al informației etc. Presupunem că o *eroare* cauzează receptarea altui simbol decît cel transmis (dar nu „pierderea" simbolului prin transmisie). Se impune găsirea unui procedeu prin care mesajul să poată ajunge în formă corectă la receptor (sau receptorul să poată detecta eventualele erori şi să ceară retransmisia mesajului).

Ideea care stă la baza teoriei *codurilor bloc corectoare de erori* este următoarea: se fixează $k, n \in \mathbb{N}^*$, cu $k < n$. Se împarte mesajul original (un şir finit de simboluri din A) în „blocuri" (numite „cuvinte") de k simboluri. Fiecărui cuvînt[76] de lungime k i se asociază un cuvînt mai lung, de lungime n, după o lege prestabilită; cele $n - k$ simboluri „în plus" sînt puse pentru detectarea şi eventual corectarea erorilor ce pot apărea în transmisie. Pe canal se transmite cuvîntul de n simboluri, la recepție urmînd ca, prin analizarea cuvîntului recepționat, să se decidă dacă au apărut erori (sau să se reconstituie cuvîntul transmis).

2.1 Exemplu. Fie $A = \{0, 1\}$ (alfabet *binar*). O idee simplă şi nu prea eficientă de codare pentru corectarea erorilor este de a transmite fiecare bit de 3 ori, urmînd ca decodarea să se facă după „regula majorității". Mai precis, luăm $k = 1$, $n = 3$ şi stabilim următorul procedeu de codare: 0 este codat ca 000, iar 1 ca 111. Astfel, dacă mesajul original este 0101, el va fi codat ca 000111000111. Să presupunem că acest mesaj este afectat de erori pe canal, încît la recepție se primeşte 001111000011. La decodare, fiecare grup de 3 biți este tratat individual: de exemplu grupul 001 este decodat în 0 (se presupune că 001 provine din 000 în care unul din 0 a devenit 1), 011 este decodat în 1 etc. Acest procedeu de corecție a erorilor funcționează atît timp cît nu apare mai mult de o eroare la fiecare grup de trei simboluri transmise.

Modelăm o situație de tipul descris, astfel: *transmițătorul* trimite un *mesaj* către *receptor* pe un *canal de transmisie*. *Mesajul* este un şir finit de *simboluri*, care sînt elemente ale unei mulțimi finite A, numită *alfabet*. Orice şir de simboluri poate fi mesaj[77]. Posibilitatea de apariție de erori pe canal este modelată de o *funcție de tranziție* $P : A \times A \to [0, 1]$, cu semnificația că $\forall x, y \in A$, $P(y, x)$ reprezintă probabilitatea ca la transmiterea simbolului x, la recepție să fie primit simbolul y.

Unul din cele mai răspîndite modele pentru un canal de transmisie este *canalul q-ar simetric de probabilitate p*: A are q elemente (este un „*alfabet q-ar*"); funcția de tranziție P are proprietatea că $P(y, x) = p$, $\forall y, x \in A$ cu $y \neq x$. Altfel spus, probabilitatea de apariție a unei

[76] Prin *cuvînt de lungime k* se înțelege un k-uplu de simboluri din A (un element din A^k).

[77] Desigur, acest lucru e fals dacă se transmit numai mesaje din limba română, de exemplu. Însă această presupunere e valabilă dacă se efecuează în prealabil o *compresie fără pierderi* a mesajului, lucru curent în practica transmisiei de date (de exemplu compresiile zip, rar, lha etc). Acest procedeu, formalizat de Huffman, se bazează pe o analiză statistică a mesajului şi codarea simbolurilor cele mai probabile în şiruri scurte şi a celor mai puțin probabile în şiruri mai lungi.

erori (simbolul primit diferă de cel trimis[78]) este $(q-1)p$, *indiferent de simbolul transmis* (de unde şi denumirea de canal *simetric*) şi *indiferent de locul simbolului în mesaj* (canal *„fără memorie”*). Deci, probabilitatea ca un simbol transmis x să fie recepționat corect este $P(x, x) = 1-(q-1)p$. Se presupune că $0 \le p < 1/2(q-1)$ (altfel este mai probabil să se recepționeze un simbol eronat decît cel corect!). Dacă $q = 2$, se vorbeşte de un canal *binar*.

Formalizăm ideea de codare bloc de mai sus: se fixează $k, n \in \mathbb{N}$, cu $k \le n$; se dă o funcție injectivă $E : A^k \to A^n$ care *codează* fiecare $a = a_1\ldots a_k \in A^k$ într-un *cuvînt cod* $c = c_1\ldots c_n \in A^n$. (Un element oarecare din A^n, $(x_1, \ldots, x_n)$, (unde $x_i \in A, \forall i$) îl scriem mai simplu $x_1\ldots x_n$.)

Mulțimea $C := E(A^k) = \{E(a_1\ldots a_k) \mid a_1\ldots a_k \in A^k\}$ a tuturor cuvintelor cod se numeşte *cod* (în cazul nostru, *cod bloc de tip* $[n, k]$). Pentru funcționarea codului trebuie dată şi o *funcție de decodare* $D : A^n \to C$, care asociază oricărui cuvînt x din A^n cuvîntul cel mai probabil transmis $D(x) \in C$. Evident, $D(c) = c, \forall c \in C$.

În acest caz, $|C| = q^k$. Este utilă şi o accepție *mai largă* a noțiunii de cod:

2.2 Definiție. Un *cod de lungime n* peste alfabetul A este o submulțime C a lui A^n. Elementele lui C se numesc *cuvinte cod*. Dacă $|A| = q$, C se numeşte *cod q-ar*.

Un cod bloc de tip $[n, k]$ transformă orice bloc de k simboluri într-un cuvînt cod de lungime mai mare n, ceea ce va permite (se speră) detecția sau corecția erorilor. Însă acest procedeu *măreşte lungimea mesajelor transmise* (ceea ce nu este de dorit). Pentru a măsura eficiența unui cod din acest punct de vedere, se defineşte *rata* de transmisie a unui cod C de tip $[n, k]$ ca fiind $R(C) := k/n$. Rata măsoară proporția de simboluri care poartă informație (restul sînt simboluri *redundante*, care folosesc la detecție sau corectare de erori). Dacă C este ca în def. 2.2, *rata* e definită ca $R(C) := \log_q|C|/n$ (de ce?).

Posibilitatea unui cod C de a corecta erori se bazează în întregime pe ideea că, dacă un cuvînt cod $c \in C$ este afectat pe canalul de transmisie de (un număr mic de) erori, cuvîntul receptat $c_t \ne c$ nu este cuvînt cod (nu aparține lui C), dar este „suficient de apropiat” de c încît să putem reconstitui c din c_t. Acest lucru este posibil doar dacă c_t nu este el însuşi un alt cuvînt cod sau nu e „mai apropiat” de alt cuvînt cod c' !

Aceste idei se pot formula riguros. Avem nevoie de cîteva pregătiri.

2.3 Definiție. Fie A o mulțime nevidă. *Distanța Hamming*[79] pe A^n se defineşte astfel:

$$\forall\, x = (x_1, \ldots, x_n),\, y = (y_1, \ldots, y_n),\ \ d(x, y) := |\{i \mid 1 \le i \le n, x_i \ne y_i\}|.$$

Deci, distanța între două cuvinte este *numărul de locuri în care cuvintele diferă*.

---

[78] Se presupune că nu "se pierd" simboluri la transmisie: numărul de simboluri transmise este egal cu numărul celor recepționate.

[79] În onoarea lui Richard Hamming (1915-1998), matematician american, fondator, alături de Shannon, al teoriei informației (articolul *Error detecting and error correcting codes*, 1950).

2.4 Propoziție. *Distanța Hamming* $d : A^n \times A^n \to \mathbb{R}$ *este o distanță (o metrică) pe* A^n, *adică:*

a) $\forall x, y \in A^n$, *avem* $d(x, y) \geq 0$;

b) $\forall x, y \in A^n$, *avem:* $d(x, y) = 0 \Leftrightarrow x = y$;

c) $\forall x, y, z \in A^n$, *avem:* $d(x, y) \leq d(x, z) + d(z, y)$.

Demonstrație. *c)* Pentru orice $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in A^n$, fie $C(x, y) := \{i \mid x_i = y_i\}$. Arătăm că $d(x, y) \leq d(x, z) + d(z, y)$, $\forall x, y, z \in A^n$. Cum $d(x, y) = n - |C(x, y)|$, inegalitatea devine: $n \geq |C(x, z)| + |C(z, y)| - |C(x, y)|$. Evident, avem $C(x, z) \bigcup C(z, y) \subseteq \{1, \ldots, n\}$, deci $|C(x, z) \bigcup C(z, y)| \leq n$, adică $|C(x, z)| + |C(z, y)| - |C(x, z) \bigcap C(z, y)| \leq n$. Însă $C(x, z) \bigcap C(z, y) \subseteq C(x, y)$, deci $n \geq |C(x, z)| + |C(z, y)| - |C(x, z) \bigcap C(z, y)| \geq |C(x, z)| + |C(z, y)| - |C(x,y)|$. □

Pentru $x \in A^n$ şi $r > 0$, *sfera (bila) de rază r centrată în x* este mulțimea cuvintelor care sînt la distanță cel mult r față de x:

$$S(x, r) := \{y \in A^n \mid d(x, y) \leq r\}.$$

Pentru $x \in A^n$, unde $|A| = q$, există $C_n^i (q-1)^i$ cuvinte aflate la distanță exact i de x. Deci:

2.5 Propoziție. *Fie* $|A| = q$. *Numărul de elemente al unei sfere de rază r din* A^n *este*

$$|S(x, r)| = \sum_{i=0}^{r} C_n^i (q-1)^i \ .$$ □

2.6 Definiție. *Distanța minimă a* unui cod $C \subseteq A^n$ este:

$$d(C) := \min \{d(x, y) \mid x, y \in C, x \neq y\}.$$

Capacitatea de corecție a codului C este:

$$e(C) := [(d(C) - 1)/2].$$

Fie C un cod cu $d(C) = d$ şi $e(C) = e = [(d - 1)/2]$. Atunci *orice două sfere centrate în cuvinte cod distincte şi de rază e sînt disjuncte* (demonstrați!). Drept consecință, dacă la transmiterea unui cuvînt cod $c \in C$ au apărut cel mult e erori, iar cuvîntul receptat este c_t, atunci $d(c, c_t) \leq e$, deci c_t *este mai aproape de c decît de orice alt cuvînt cod.*

Pentru a găsi c, plecînd de la c_t, se poate folosi un *algoritm de distanță minimă*, adică un algoritm care, dat un cuvînt $x \in A^n$, găseşte un cuvînt cod $w_x \in C$ care este cel mai aproape de x, adică $d(x, w_x) = \min \{d(x, y) \mid y \in C\}$.

2.7 Observație. Utilizarea unui cod C de lungime n, distanță minimă d şi capacitate de corecție e se poate face în două moduri distincte:

- modul „corectare de erori": se presupune că orice bloc de n simboluri c este afectat de cel mult e erori. Dacă cuvîntul recepționat este c_t, c_t poate fi decodat în mod univoc în c. [80]

[80] De aici şi denumirea de *capacitate de corecție a lui C* ce se dă lui *e*.

- modul „detectare de erori”: se presupune că la transmiterea oricărui bloc de n simboluri apar cel mult $d-1$ erori. Atunci nici un cuvînt cod c nu poate fi transformat pe parcursul transmiterii în alt cuvînt cod c'. Astfel, dacă receptorul primeşte un cuvînt c_t care nu este cuvînt cod, semnalează „eroare” (şi cere eventual retransmiterea cuvîntului).

2.8 Exercițiu. a) Demonstrați afirmațiile din observația de mai sus.

b) Arătați că există două sfere centrate în cuvinte cod distincte şi de rază $e+1$ care nu sînt disjuncte. În consecință, există o situație în care un cuvînt afectat de $e+1$ erori nu este decodat corect prin algoritmul de distanță minimă.

În general, teoria codurilor bloc corectoare de erori se poate dezvolta pentru acele coduri C care au o anumită *structură*. O astfel de situație este cea în care *alfabetul este un corp finit F* (cu q elemente[81], unde q este o putere a unui număr prim), iar codul $C \subseteq F^n$ este *subspațiu liniar* în F^n. Deşi aceste condiții limitează drastic clasa codurilor pe care le studiem, această clasă este suficient de largă pentru a furniza coduri importante şi eficiente, folosite pe scară largă în practică. În continuare presupunem că cititorul este familiarizat cu noțiuni şi rezultate elementare de Algebră Liniară: spațiu liniar, dependență liniară, sistem de generatori, baze, dimensiune, produsul scalar standard în F-spațiul liniar F^n.

2.9 Definiție. Fie F un corp finit cu q elemente. Se numeşte *cod liniar* de lungime n peste F orice subspațiu liniar C al lui F^n. Cu alte cuvinte, C este o mulțime de cuvinte de lungime n în care simbolurile sînt elemente din F, închisă la adunarea (pe componente) din F^n şi la înmulțirea cu scalari din F.[82]

Dimensiunea codului liniar C este dimensiunea lui C ca spațiu liniar peste F. Dacă $\dim C = k$ şi distanța minimă a lui C este d, spunem că C este cod liniar *de tip* $[n, k, d]_q$ (sau *cod liniar q-ar de tip* $[n, k, d]$); n, k, d se numesc *parametrii* codului C.

Corpul finit cu q elemente este notat cu $\mathbb{F}_q$.

2.10 Exemplu. Codul „de repetiție de 3 ori” din exemplul 2.1 este $C = \{000, 111\}$, care este subspațiu în $\mathbb{F}_2^3$. Distanța minimă a lui C este 3, deci C este un cod liniar binar de tip $[3, 1, 3]_2$. Astfel, $e(C) = 1$, ceea ce a fost deja remarcat.

Pentru un cod C dat, determinarea distanței minime este foarte importantă. A priori, pentru aceasta ar trebui să considerăm toate distanțele $d(x, y)$ cu $x, y \in C$ distincte, adică $|C|\cdot(|C|-1)/2$ distanțe, ceea ce este practic inabordabil (la codurile Reed-Solomon folosite în CD-uri, $|C|$ este de ordinul 2^{224}). La coduri *liniare*, avem deja o sarcină uşurată:

---

[81] Foarte adesea, F este $\mathbb{F}_2$, corpul cu două elemente.

[82] Condiția ca C să fie parte stabilă la înmulțirea cu scalari este redundantă pentru cazul corpului cu două elemente. De ce? Mai puteți da exemple de corpuri pentru care se întîmplă acelaşi fenomen?

2.11 Propoziție. *Fie F un corp finit. Atunci distanța Hamming pe F^n este invariantă la translații:* $d(x, y) = d(x + z, y + z)$, $\forall x, y, z \in F^n$. *În particular,* $d(x, y) = d(x - y, 0)$ *şi deci distanța minimă a unui cod liniar* $C \leq F^n$ *este:*

$$d(C) = \min\{d(x, 0) \mid x \in C, x \neq 0\}. \qquad \square$$

Ponderea (*Hamming*) $\mathrm{wt}(x)$ a unui cuvînt (vector) $x = x_1 \ldots x_n \in F^n$ se defineşte ca numărul coordonatelor sale nenule (echivalent, $\mathrm{wt}(x) = d(x, 0)$)[83]. Deci, *distanța minimă a unui cod liniar este ponderea minimă nenulă a cuvintelor cod*.

Cum putem preciza în mod concret un cod liniar? Există două moduri naturale de a da un subspațiu liniar C (un cod liniar) de dimensiune k în F^n: se dă o *bază* a lui C (adică se dau k *vectori liniar independenți în* C) sau se descrie C ca *mulțimea soluțiilor unui sistem omogen de* $n - k$ *ecuații liniar independente*:

2.12 Definiție. Fie $C \leq F^n$ un cod liniar de dimensiune $k \leq n$ peste corpul F. O *matrice generatoare* a lui C este o matrice $G \in \mathrm{M}(k, n, F)$ ale cărei *linii* (văzute ca vectori în F^n) formează o bază în C (deci liniile lui G sînt liniar independente, adică rang $G = k$).

O *matrice de paritate*[84] a lui C este o matrice $H = (h_{ij}) \in \mathrm{M}(n - k, n, F)$ astfel încît, $\forall x = (x_1, \ldots, x_n) \in F^n$:

$$x \in C \Leftrightarrow h_{i1}x_1 + \ldots + h_{in}x_n = 0,\ 1 \leq i \leq n - k.$$

Deci, pentru ca H să fie o matrice de paritate pentru codul C de dimensiune k, trebuie ca rang $H = n - k$ şi să aibă loc: $x \in C \Leftrightarrow Hx^T = 0 \in \mathrm{M}(n - k, 1, F)$.

2.13 Observație. Denumirea de *matrice de paritate* (*parity-check matrix*) provine din cazul particular al codului binar următor: se fixează $k \in \mathbb{N}^*$ şi orice vector $x_1 \ldots x_k \in \mathbb{F}_2^{\,k}$ este codat ca $x_1 \ldots x_k x_{k+1}$, unde x_{k+1} este astfel încît $x_1 + \ldots + x_k + x_{k+1} = 0$ (în $\mathbb{F}_2$). Codul este aşadar $C = \{x_1 \ldots x_k x_{k+1} \in \mathbb{F}_2^{\,k+1} \mid x_1 + \ldots + x_k + x_{k+1} = 0\}$. Orice cuvînt cod are un număr par de biți egali cu 1 şi de aceea bitul x_{k+1} este numit *bit de paritate*. Verificarea faptului că un cuvînt x este cuvînt cod revine la a verifica „paritatea” cuvîntului, adică un tip particular de sistem liniar omogen pe care îl satisfac coordonatele lui x. Determinați parametrii acestui cod!

Fie $\langle x, y\rangle = x_1y_1 + \ldots + x_ny_n$, $\forall x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in F^n$ *produsul scalar standard* pe F^n; dacă $S \subseteq F^n$, fie $S^\perp := \{y \in F^n \mid \langle x, y\rangle = 0, \forall x \in S\}$ *ortogonalul* lui S (doi vectori x, $y \in F^n$ se numesc *ortogonali* sau *perpendiculari* dacă $\langle x, y\rangle = 0$). Lăsăm ca exercițiu demonstrarea proprietăților următoare:

2.14 Teoremă. *Fie C un cod liniar de tip* $[n, k, d]$ *peste corpul F. Atunci:*

---

[83] Notația *wt* vine de la *weight* (greutate, pondere).
[84] Se mai folosşte terminologia "matrice de control".

a) $C^{\perp}$ *este un cod liniar de dimensiune* $n - k$ (numit *codul dual lui* C).

b) $(C^{\perp})^{\perp} = C$.

c) Dacă G este o matrice generatoare a lui C, atunci G este o matrice de paritate pentru $C^{\perp}$*. Dacă H este matrice de paritate pentru C, atunci H este matrice generatoare pentru* $C^{\perp}$.□

Folosind noțiunea de ortogonalitate putem spune: $H \in \mathrm{M}(n - k,\ n,\ F)$ *este matrice de paritate pentru codul* $C \leq F^n \Leftrightarrow$ *liniile lui H sînt liniar independente și C este mulțimea vectorilor ortogonali pe liniile lui H* (*văzute ca vectori în* F^n).

Observăm că un vector nenul în F^n poate fi ortogonal pe el însuşi (de ex. $(1, 1)$ în $\mathbb{F}_2^{\,2}$), deci este posibil ca C şi $C^{\perp}$ să aibă intersecție nenulă[85]. Dacă $C = C^{\perp}$, C se numeşte *autodual*. Distanța minimă a unui cod liniar poate fi citită de pe matricea sa de paritate:

2.15 Teoremă. *Fie C un cod liniar peste F și* $H \in \mathrm{M}(n - k, n, F)$ *o matrice de paritate pentru C. Atunci distanța minimă d a lui C este*

$$d = \min\{\delta \mid \text{există } \delta \text{ coloane în } H \text{ care sînt liniar dependente}\}.$$

Demonstrație. Fie $H_i \in F^{n-k}$ coloana i a lui H, $1 \leq i \leq n$. Avem $(x_1, \dots, x_n) \in C$ dacă şi numai dacă $x_1H_1 + \dots + x_nH_n = 0$. Fie $d' = \min\{\delta \mid \text{există } \delta \text{ coloane în } H, \text{ liniar dependente}\}$.

Fie $(x_1, \dots, x_n) \in C$, de pondere minimă d. Atunci coloanele H_i pentru care $x_i \neq 0$ (în număr de d) sînt liniar dependente, deci $d' \leq d$. Reciproc, fie o mulțime de d' coloane $\{H_i\}_{i \in J}$, liniar dependentă. Atunci există $(x_1, \dots, x_n) \in F^n$ cu $x_1H_1 + \dots + x_nH_n = 0$ şi $x_i \neq 0 \Rightarrow i \in J$. Deci $x = (x_1, \dots, x_n) \in C$ şi $d \leq \mathrm{wt}(x) \leq d'$. □

Observăm că avem şi

$$d = 1 + \max\{m \in \mathbb{N} \mid \text{orice } m \text{ coloane în } H \text{ sînt liniar independente}\}.$$

O clasă importantă de coduri corectoare de erori a fost descoperită de Hamming.

2.16 Definiție. (Coduri Hamming) Fie $F = \mathbb{F}_q$ şi $r \in \mathbb{N}^*$ fixat. Definim *codul Hamming q-ar de redundanță r*, $H_{q,\,r}$, astfel:

Construim o matrice de paritate H care să aibă orice 2 coloane liniar independente, dar există 3 liniar dependente (deci distanța minimă a codului va fi 3). Alegem cîte un vector nenul din fiecare subspațiu de dimensiune 1 din F^r; construim matricea H ce are drept coloane aceşti vectori (într-o ordine arbitrară). Matricea H este prin definiție matricea de paritate H a codului $H_{q,\,r}$.

Un alt mod de a exprima ideea de mai sus este: pe $F^r \setminus \{0\}$ definim o relație de echivalență: $x \sim y \Leftrightarrow \exists \alpha \in F^*$ astfel încît $y = \alpha \cdot x$. Din fiecare clasă de echivalență alegem cîte un vector[86]. Aceşti vectori sînt coloanele matricei de paritate H.

---

[85] Adică, deşi $\dim C + \dim C^{\perp} = n$, nu are loc în general $C \oplus C^{\perp} = F^n$. Ce puteți spune dacă F este de caracteristică 0?

Cîte coloane are H ? Se observă că clasele de echivalență de mai sus au fiecare cîte $q-1$ elemente (clasa de echivalență a lui $x \in F^r \setminus \{0\}$ este $\{\alpha x \mid \alpha \in F^*\}$). Cum reuniunea lor (disjunctă) este $F^r \setminus \{0\}$, avem $q^r - 1 = n(q-1)$, unde n este numărul claselor de echivalență.

Deci H are $n = (q^r - 1)/(q-1)$ coloane şi r linii.

Pentru ca $H \in \mathrm{M}(r, n, K)$ să fie matrice de paritate, trebuie ca rang $H = r$. Există într-adevăr r coloane liniar independente în H, de exemplu (multipli scalari de) $(1, 0, \ldots, 0)^T$, $(0, 1, \ldots, 0)^T$, $\ldots$, $(0, 0, \ldots, 1)^T$.

2.17 Observație. Construcția de mai sus nu determină în mod unic matricea de paritate H. De exemplu, pentru două ordonări diferite ale coloanelor se obțin două matrice de paritate H, H' distincte şi deci coduri Hamming corespunzătoare *distincte* C, C'. Însă aceste coduri sînt *echivalente pînă la o permutare*, în sensul că $\exists \sigma \in S_n$ (grupul permutărilor mulțimii $\{1, 2, \ldots, n\}$) astfel încît $\forall x_1\ldots x_n \in F^n$, avem $x_1\ldots x_n \in C \Leftrightarrow x_{\sigma(1)}\ldots x_{\sigma(n)} \in C'$.

Dacă în matricea de paritate H a codului Hamming C se înlocuieşte coloana i (fie aceasta P_i) cu coloana αP_i, unde $\alpha \in F^*$, atunci se obține o matrice H', de paritate pentru un cod C' astfel încît avem $x_1\ldots x_i\ldots x_n \in C \Leftrightarrow x_1\ldots(\alpha^{-1}x_i)\ldots x_n \in C$.

Această situație sugerează definirea unui alt tip de echivalență: două coduri C, C' de lungime n peste corpul F se numesc *diagonal echivalente* dacă $\exists\ (\alpha_1, \ldots, \alpha_n) \in (F^*)^n$ astfel încît $\forall (x_1,\ldots, x_n) \in F^n$, avem $(x_1,\ldots, x_n) \in C \Leftrightarrow (\alpha_1 x_1,\ldots, \alpha_n x_n) \in C'$. Două coduri C, C' care sînt echivalente (diagonal sau pînă la o permutare) au în esență „aceleaşi”[87] proprietăți: de exemplu, C este liniar $\Leftrightarrow C'$ este liniar.

Reuniunea celor două relații de echivalență pentru coduri de lungime n peste F se numeşte *echivalență monomială*. Deci, *codul Hamming $H_{q,r}$ este unic determinat pînă la o echivalență monomială*.

2.18 Exemplu. (codul binar Hamming [7, 4, 3]) Pentru $q = 2$ şi $r = 3$, avem $n = 7$ şi H este:

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

În cazul $F = \mathbb{F}_2$, coloanele lui H sînt unic determinate pînă la o ordine a lor (fiecare subspațiu de dimensiune 1 din F^r are exact un vector nenul). Ordinea coloanelor adoptată aici este cea lexicografică (altfel spus, am scris „pe verticală” toate numerele nenule de 3 cifre în baza 2, în ordinea lor naturală). Acest cod are o importanță istorică deosebită:

Studiile superioare ale lui Hamming erau de matematică pură, iar teza sa de doctorat era despre ecuații diferențiale. A făcut parte din "Manhattan Project", proiectul ultrasecret de fabricare a bombei atomice de la Los Alamos din timpul celui de al doilea război mondial. În 1946 a plecat de la Los Alamos la Bell Laboratories :

---

[86] Se vede o legătură strînsă cu *spațiile proiective*.

[87] Enunțați cît mai multe proprietăți ale unui cod care se conservă prin echivalențele definite aici. Puteți defini şi alte tipuri de echivalențe?

I was a pure mathematician – I felt somewhat lost at the place. Every once in a while I got terribly discouraged at the department being mostly electrical engineering.

La Bell Labs aveau un computer Model V, care ocupa 90 metri pătrați, cîntărea 10 tone şi putea rezolva sisteme liniare de 13 ecuații în mai puțin de 4 ore. Hamming avea acces doar în weekend la computer; cum nu exista personal de supraveghere în weekenduri, dacă computerul descoperea o eroare, abandona pur şi simplu sarcina şi trecea la următoarea.

Two weekends in a row I came in and found that all my stuff had been dumped and nothing was done. I was really aroused and annoyed because I wanted those answers and two weekends had been lost. And so I said "Damn it, if the machine can detect an error, why can't it locate the position of the error and correct it?"

Codul pe care l-a descoperit Hamming este chiar codul binar tip [7, 4, 3] de mai sus, care poate corecta o eroare la 7 simboluri. Nu este totdeauna de dorit să obținem coduri care să corecteze cît mai multe erori, deoarece rata de transmisie ar putea fi prea mică sau decodarea ar putea consuma prea mult timp. Este necesară obținerea de coduri suficient de bune pentru o anumită sarcină. Hamming spunea în legătură cu aceasta:

The Relay Computer, operating with a self-checking code, stops whenever an error is detected. Under normal operating conditions this amounts to two or three stops per day. However, if we imagine a comparable electronic computing machine operating 10^5 *times the speed and with elements* 10^3 *times more reliable than relays, we find two to three hundred stops per day.*

Putem spune că Hamming a prevăzut apariția atît a computerelor rapide de astăzi, cît şi a sistemelor de operare Windows.

Să descriem o modalitate practică de codare şi de decodare pentru acest cod $H_{2,3}$. Întrucît este un cod tip [7, 4], fiecare mesaj de 4 biți este codat pe un cuvînt cod de 7 biți. Coordonatele unui cuvînt cod $d = d_1 \dots d_7 \in H_{2,3}$ satisfac ecuația $Pd^{\mathrm{T}} = 0$, adică

$$\begin{aligned} d_1 + d_3 + d_5 + d_7 &= 0 \\ d_2 + d_3 + d_6 + d_7 &= 0 \\ d_4 + d_5 + d_6 + d_7 &= 0 \end{aligned} \qquad (*)$$

Alegem biții d_1, d_2, d_4 să fie „de control”, iar biții mesajului original sînt plasați în pozițiile 3, 5, 6, 7. Biții d_1, d_2, d_4 se obțin din ecuațiile de mai sus, adică $d_1 = d_3 + d_5 + d_7$ etc.[88]

La recepția unui cuvînt de 7 biți $r = r_1 \dots r_7$, se verifică dacă r este cuvînt cod (adică dacă $r_1, \dots, r_7$ satisfac ecuațiile (*)). Altfel spus, se calculează $(c_1, c_2, c_3) = H(r_1, \dots, r_7)^T$. Dacă $(c_1, c_2, c_3) = (0, 0, 0)$, atunci nu au avut loc erori. Dacă $(c_1, c_2, c_3) \neq (0, 0, 0)$, atunci eroarea (presupusă a fi singura) e plasată în bitul a cărui poziție este dată de numărul binar $c_3c_2c_1$ (şi deci poate fi corectată!).[89]

2.19 Propoziție. *Fie* $F = \mathbb{F}_q$ şi $r \in \mathbb{N}^*$. *Atunci codul Hamming* $H_{q,r}$ *este un cod liniar de lungime* $n = (q^r - 1)/(q - 1)$, *dimensiune* $n - r$ *şi distanță minimă* 3.

Demonstrație. Rămîne să vedem că distanța minimă este 3. Este clar că putem alege 3 coloane liniar dependente în H, de exemplu $(1, 0, \dots, 0)^T$, $(0, 1, \dots, 0)^T$, $(1, 1, \dots, 0)^T$, (ultima este suma primelor două). Orice două coloane sînt liniar independente din construcție. □

2.20 Teoremă (inegalitatea Hamming). *Fie C un cod q-ar de lungime n cu capacitate de corecție e. Atunci*

[88] De ce s-a ales astfel poziția biților de control?

[89] Justificați această procedură de decodare!

$$|C|\sum_{i=0}^{e} C_n^i (q-1)^i \le q^n.$$

Demonstrație. Sînt q^n elemente în A^n şi $|C|$ cuvinte cod în C. Sferele de rază e centrate în cuvintele cod sînt disjuncte două cîte două, deci $|C|\cdot|S(x, e)| \le q^n$. Se aplică propoziția 2.5. □

Pentru orice cod C (nu neapărat liniar) de capacitate de corecție e, sferele centrate în cuvintele cod de rază e sînt disjuncte; dacă reuniunea lor este întreg F^n, atunci codul se numeşte (e-)*perfect*. Echivalent, *un cod este perfect dacă are loc egalitate în inegalitatea Hamming.*

2.21 Exercițiu. Orice cod e-perfect are distanță minimă $2e + 1$.

Codurile Hamming sînt 1-*perfecte* (verificați!). Altfel spus, orice cuvînt din F^n se găseşte la distanță ≤ 1 de exact un cuvînt cod. Acest fenomen are aplicații oarecum surprinzătoare.

2.22 Aplicație. *Jocul Pronosport* constă în ghicirea rezultatelor a 13 partide de fotbal. Rezultatul unei partide este un element al mulțimii {x, 1, 2} (x = egalitate; 1 = cîştigă gazdele; 2 = cîştigă oaspeții). Jucătorii completează *variante*; numim variantă orice 13-uplu $(s_1,\dots, s_{13})$, cu $s_i \in \{x, 1, 2\}$. Pentru a cîştiga cu siguranță premiul I (13 rezultate exacte), este necesară a priori completarea a 3^{13} variante. Se pune întrebarea: *care este numărul minim de variante ce trebuie completate pentru a cîştiga cu siguranță premiul* II (12 *rezultate exacte*)?

Reformulăm problema în termenii teoriei codurilor: *Fie* $F = \mathbb{F}_3$, *corpul cu* 3 *elemente. Să se găsească o submulțime* (*un cod*) $S \subseteq F^{13}$ (*cît mai „mică”*), *astfel încît orice cuvînt din* F^{13} *să se găsească la distanță cel mult* 1 *de un cuvînt din S. Altfel spus, să se găsească un cod* 1-*perfect de lungime* 13 *peste* $\mathbb{F}_3$.

Răspunsul este dat de codul Hamming cu $q = 3$ şi $r = 3$: avem $n = (3^3 - 1)/2 = 13$, deci este un cod tip $[13, 10, 3]_3$. Numărul de cuvinte cod (de „variante”) este $3^{10} = 59049$.

2.23 Exercițiu. Scrieți o matrice de paritate pentru codul Hamming de mai sus.

2.24 Aplicație. *Problema pălăriilor*. Se dă o echipă de 3 persoane care joacă următorul joc: în mod aleator, pe capul fiecărei persoane se pune o pălărie roşie sau albastră, fără ca persoana să ştie culoarea pălăriei. În schimb, fiecare poate vedea pălăriile tuturor celorlalți. Fiecare persoană ghiceşte culoarea pălăriei proprii sau se abține (spune „pas”). Echipa cîştigă dacă toate persoanele care au ghicit, au ghicit corect. Dacă toată lumea s-a abținut, echipa pierde.

Membrii echipei nu au voie să comunice între ei după ce au primit pălăriile; în schimb, pot stabili o strategie înaintea jocului.

Se pune problema de a determina o strategie optimă şi probabilitatea de cîştig a echipei cu această strategie. O strategie evidentă, cu 50% şanse de cîştig, este de a desemna un membru al echipei care să ghicească la întîmplare, iar restul să se abțină. Se poate mai bine?

Pentru aceasta, să definim cîteva noțiuni relativ la acest joc. Considerăm cazul mai general a n persoane, iar mulțimea culorilor o considerăm $C = \{0, 1\}$ (0 = roşu, 1 = albastru).

Să numerotăm persoanele de la 1 la n. Fiecare persoană i ghiceşte în funcție de configurația de pălării pe care o vede la ceilalți. Vom defini deci :

- o *configurație* este un n-uplu de culori, adică un element $(x_1, \ldots, x_n) \in C^n$.

- o *strategie* este o familie de funcții $\varphi = (\varphi_i)_{1 \le i \le n}$, cu $\varphi_i : C^{n-1} \to \{0, 1, pas\}$, cu sensul că: persoana i declară $\varphi_i(x_1, \ldots, \widehat{x_i}, \ldots, x_n)$, pentru o configurație dată $(x_1, \ldots, x_n)$ (am notat cu $(x_1, \ldots, \widehat{x_i}, \ldots, x_n)$ faptul că x_i este omis din n-uplul $(x_1, \ldots, x_n)$).

- configurația $(x_1, \ldots, x_n) \in C^n$ este *configurație cîştigătoare pentru strategia* $(\varphi_i)_{1 \le i \le n}$ dacă există i astfel încît $\varphi_i(x_1, \ldots, \widehat{x_i}, \ldots, x_n) = x_i$.

- *mulțimea cîştigătoare pentru strategia* $\varphi = (\varphi_i)_{1 \le i \le n}$ este $W_\varphi = \{(x_1, \ldots, x_n) \in C^n \mid (x_1, \ldots, x_n)$ este configurație cîştigătoare pentru $\varphi\}$.

Pentru $n = 3$, să considerăm următoarea strategie: dacă persoana i ($i \in \{1, 2, 3\}$) vede două pălării identice, ghiceşte culoarea opusă; dacă nu, spune *pas* [90]. Configurațiile posibile sînt toate tripletele de forma 000, 001, …, 111 (în număr de 8). Configurațiile în care se *pierde* sînt 000 şi 111 (de ce?). Orice altă configurație este cîştigătoare pentru această strategie (de ce?). Astfel, probabilitatea de cîştig este: (numărul cazurilor favorabile)/(numărul total de cazuri) = $1 - 2/8 = 0{,}75$.

Observăm că mulțimea configurațiilor pierzătoare este chiar codul Hamming binar $H_{2,\,2}$, de tip [3, 1, 3]. Acest lucru nu este întîmplător.

În cazul general, este esențial următorul rezultat: Fie $W \subseteq C^n$. Atunci există o strategie φ astfel încît W este mulțime cîştigătoare pentru φ dacă şi numai dacă $P := C^n \setminus W$ are proprietatea:

$$\forall x \notin P,\ \exists x' \in P \text{ astfel încît } d(x, x') = 1. \qquad \text{(P)}$$

Cu d s-a notat distanța Hamming. Proprietatea (P) înseamnă că: $\forall x = (x_1, \ldots, x_n) \notin P$, există un i astfel încît, modificînd x_i (în $1 - x_i$), se obține cuvîntul $(x_1, \ldots, 1 - x_i, \ldots, x_n) \in P$.

<u>Demonstrație</u>. Presupunem W cîştigătoare pentru φ. Fie $x = (x_1, \ldots, x_n) \notin P$. Deci $x \in W$, adică $\exists i$ astfel încît $\varphi_i(x_1, \ldots, \widehat{x_i}, \ldots, x_n) = x_i$. Atunci $\varphi_i(x_1, \ldots, \widehat{1 - x_i}, \ldots, x_n) = \varphi_i(x_1, \ldots, \widehat{x_i}, \ldots, x_n) = x_i \neq 1 - x_i$, deci $x' := (x_1, \ldots, 1 - x_i, \ldots, x_n) \in P$, iar $d(x, x') = 1$.

Fie acum P cu proprietatea enunțată. Definim strategia $\varphi = (\varphi_i)_{1 \le i \le n}$ astfel:

Pentru $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \in C^{n-1}$, $\varphi_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = \varepsilon$, unde ε este definit astfel:

- dacă $\exists x_i \in \{0, 1\}$ astfel încît $(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n) \in P$, atunci $\varepsilon = 1 - x_i$.
- *pas*, în caz contrar.

[90] Definiți funcțiile φ_i pentru acest caz!

Demonstrăm că $W = C^n \setminus P$ este mulțime cîştigătoare pentru φ. Fie $x = (x_1, \ldots, x_n) \notin P$. Din proprietatea (P), există un i astfel încît $(x_1, \ldots, 1 - x_i, \ldots, x_n) \in P$. Atunci, conform strategiei de mai sus, $\varphi_i(x_1, \ldots, \widehat{x_i}, \ldots, x_n) = 1 - 1 + x_i = x_i$. □

Astfel, a da o strategie φ revine la a da o mulțime P (o putem numi *pierzătoare* pentru φ) cu proprietatea (P). Pentru ca stragtegia să fie optimă, trebuie ca mulțimea cîştigătoare $W = C^n \setminus P$ să fie cît mai mare, deci P să fie cît mai mică. Astfel, a găsi strategii optime revine la a găsi mulțimi P cu proprietatea (P), care să fie cît mai mici. Proprietatea (P) spune că reuniunea sferelor centrate în cuvintele din P, de rază 1, acoperă C^n. *Altfel spus, să se găsească un cod* 1-*perfect de lungime n peste* $C = \mathbb{F}_2$. Se vede analogia cu problema jocului Pronosport.

Pentru n de forma $2^r - 1$, o soluție este dată de codul Hamming $H_{2,\,r}$. Acest cod, de tip $[n, n - r, 3]$ are 2^{n-r} cuvinte, deci probabilitatea de cîştig este $1 - 2^{n-r}/2^n = 1 - 2^{-r}$. De exemplu, pentru $n = 7$, probabilitatea este $1 - 2^{-3} = 7/8$.

O altă familie de coduri cu aplicații practice importante este următoarea.

2.25 Definiție (coduri Reed-Solomon)**.** Fie q o putere a unui prim şi $F = \mathbb{F}_q$. Fixăm un element primitiv $\alpha \in F^*$, (deci $F \setminus \{0\} = \{1, \alpha, \ldots, \alpha^{q-2}\}$, α este de ordin $q - 1$ în F^*) şi k, $1 \le k \le q - 1$. Codul *Reed-Solomon* $RS(k, q)$ este:

$$RS(k, q) := \{(f(1), \ldots, f(\alpha^{q-2})) \in F^{q-1} \mid f \in F[X], \deg f \le k - 1\}$$

Se observă că $RS(k, q)$ este cod de lungime $n = q - 1$ peste F. Notăm

$$L_{k-1} := f \mid f \in F[X], \operatorname{gr} f \le k - 1\}$$

L_{k-1} este un subspațiu liniar în $F[X]$, de dimensiune k. Atunci $RS(k, q)$ este imaginea aplicației de evaluare $ev : L_{k-1} \to F^{q-1}$, $ev(f) = (f(1), \ldots, f(\alpha^{q-2}))$, care este evident liniară, deci $RS(k, q)$ este subspațiu liniar în F^{q-1}. Avem $\dim RS(k, q) = k$, căci ev este injectivă (orice $f \in L_{k-1}$ cu $ev(f) = (0, \ldots, 0)$ are $q - 1 > \operatorname{gr} f$ rădăcini şi deci este 0). Ponderea (distanța) minimă a lui $RS(k, q)$ este $d = q - k = n - k + 1$ (exercițiu!), adică are loc egalitate în inegalitatea de mai jos:

2.26 Teoremă. (inegalitatea Singleton) *Fie C un cod de lungime n şi distanță minimă d peste un alfabet A cu q simboluri. Atunci* $|C| \le q^{n-d+1}$. *Dacă C este liniar, atunci* $d \le n - k + 1$.

Demonstrație. Rezultă din faptul că, pentru $(x_1, \ldots, x_{n-d+1}) \in A^{n-d+1}$ fixat, există cel mult un cuvînt cod în C ale cărui coordonate de pe primele $n - d + 1$ locuri sînt $(x_1, \ldots, x_{n-d+1})$ (justificați!). □

Codurile liniare pentru care $d = n - k + 1$ se numesc *coduri MDS* (*Maximum Distance Separable*) şi sînt „cele mai bune” dintr-un anumit punct de vedere (distanța minimă a codului este maxim posibilă dacă dimensiunea şi lungimea codului sînt fixate).

Codurile Reed-Solomon (*RS*) sînt deci MDS. Vom arăta că ele sînt adaptate la transmisia pe canale afectate de *pachete de erori* (în engleză *burst errors*): erorile apar mai probabil unele după altele (în „pachete”). Această situație apare adesea în practică, de pildă la stocarea datelor pe bandă sau CD (o zgîrietură pe CD afectează un şir de biți succesivi), comunicații radio etc.

Presupunem că mesajul inițial (necodat) este o succesiune de cuvinte de cîte k simboluri binare. Alegem un t astfel încît $q := 2^t > k$, punem F = corpul cu q elemente şi folosim un cod $RS(k, q)$. Cum $|F| = 2^t$, există o bijecție între F şi $\{0, 1\}^t$; putem atunci ca în fiecare cuvînt cod $c = (x_1, \ldots, x_{q-1}) \in RS(k, q) \subseteq F^{q-1}$ să considerăm x_i ca un cuvînt de t cifre binare. Astfel, cuvîntul cod $c = (x_1, \ldots, x_{q-1}) \in F^{q-1}$ este transmis ca un cuvînt binar w de lungime $t(q-1)$. Un pachet de b erori în cuvîntul binar w corespunde unui pachet de b/t erori în c, care poate fi corectat dacă $b/t \le e$, unde $e = [(q - k - 1)/2]$ este capacitatea de corecție a codului.

De exemplu, alegînd $k = 240$, $t = 8$, $q = 2^8 = 256$, $d = 16$, $e = 7$, se pot corecta pachete de 56 biți eronați. Prin tehnici de *concatenare* şi *întrețesere*, se ajunge în practică la posibilitatea de corecție a circa 4000 erori binare (corespunzînd unei lungimi pe CD de 2,5 mm).

Teoria codurilor corectoare de erori este mult mai vastă decît am putut schița aici. Este un domeniu dinamic, în care se regăsesc în mod spectaculos şi alte ramuri ale matematicii precum geometria algebrică, combinatorica, teoria grafurilor etc.

Exerciții

1. Fie F un corp cu q elemente, $n \in \mathbb{N}$ şi $m < q^n$. Cîte coduri de lungime n peste F cu m cuvinte există? Cîte din acestea sînt liniare? (*Ind.* Dacă m nu este de forma q^k, nu există subspații liniare cu m elemente în F^n. Dacă $m = q^k$, trebuie găsit numărul subspațiilor liniare de dimensiune k din F^n.)

2. (Coduri de repetiție) Considerăm următorul procedeu de codare: pentru a coda cuvinte oarecare de lungime k (peste alfabetul binar $\{0, 1\} = F$) se repetă fiecare bit de r ori; astfel, orice cuvînt $x_1 \ldots x_k$ este codat ca $x_1 \ldots x_1 x_2 \ldots x_2 \ldots x_k \ldots x_k$ (fiecare x_i apare de r ori). Se obține un cod de lungime kr.

a) Arătați că acest cod este liniar, de dimensiune r.

b) Arătați că distanța sa minimă este r.

c) Folosim codul de repetiție de tip [3,1]. Dacă se primeşte mesajul 000101111100, unde au apărut erori? Corectați-le.

d) Care este rata de transmisie a codului de repetiție tip $[kr, r]$?

3. Scrieți toate cuvintele codului Hamming $H_{2,2}$, Care este rata sa de transmisie?

4. Scrieți toate cuvintele codului binar Hamming tip [7, 4, 3]. Care este rata sa de transmisie?

5. Calculați numărul de cuvinte şi rata de transmisie ale codului Hamming $H_{q,\,r}$ (în general) şi pentru $q = 2$, $r \le 5$.

6. Fie C un cod liniar de tip $[n, k, d]$ peste F, corp cu q elemente.

a) Arătați că: ori toate cuvintele din C încep cu 0, ori exact $1/q$ din cuvinte încep cu 0. (*Ind.* Fie $D := \{x_1\ldots x_n \in F^n \mid x_1 = 0\}$, subspațiu liniar în F^n. Aplicați formula pentru $\dim(C + D)$).

b) Demonstrați că suma ponderilor tuturor cuvintelor lui C este cel mult $n(q-1)q^{k-1}$.

c) Demonstrați că $d \le \dfrac{n(q-1)q^{k-1}}{q^k - 1}$. (*Ind.* Distanța minimă este mai mică decit media ponderilor cuvintelor nenule.)

d) (Inegalitatea Plotkin) Demonstrați că, dacă $\dfrac{d}{n} > \dfrac{q-1}{q}$, atunci $|C| \le \dfrac{d}{d - \frac{q-1}{q}n}$.

7. Demonstrați că dualul unui cod liniar MDS este tot cod MDS.

8. Demonstrați că un cod *binar* MDS de lungime n este unul din următoarele: un cod de repetiție, codul de paritate sau tot spațiul $\mathbb{F}_2{}^n$.

VI. Acțiuni ale grupurilor

VI.1. Acțiuni ale grupurilor pe mulțimi

Conceptul de grup este strîns legat de noțiunea de *acțiune*. Cauchy are ideea de a privi substituțiile (permutările) unei mulțimi ca obiecte în sine şi observă că aceste substituții se pot compune. Lagrange studiase deja comportarea polinoamelor la permutarea nedeterminatelor; mai precis, „acțiunea” unei permutări a nedeterminatelor asupra unui polinom dat. Galois duce această idee mai departe şi o utilizează în studiul rezolvabilității ecuațiilor polinomiale, studiind acțiunile permutărilor asupra rădăcinilor ecuației. Tot la Galois apare utilizarea termenului de *grup* de permutări şi folosirea unui singur simbol pentru a nota o permutare.

1.1 Exemplu. Fie polinomul (în 4 nedeterminate) $p = X_1 + X_2 + X_3 + X_4$. Oricum am permuta cele 4 nedeterminate, polinomul p rămîne acelaşi. În schimb, pentru $q = X_1X_2 + X_3X_4$, putem obține prin permutarea nedeterminatelor polinoamele: $X_1X_3 + X_2X_4$, $X_1X_4 + X_2X_3$ şi, bineînțeles, polinomul inițial $X_1X_2 + X_3X_4$.

Lagrange a demonstrat că, pentru orice polinom p de n nedeterminate, numărul polinoamelor ce se pot obține din p prin permutarea nedeterminatelor este un divizor al lui $n!$. Vom vedea că acest enunț este un caz particular al cunoscutei teoreme (numită chiar „Teorema lui Lagrange”): *ordinul oricărui subgrup al unui grup finit divide ordinul grupului*.

1.2 Definiție. Fie $(G,\cdot)$ un grup, e elementul său unitate şi X o mulțime. Spunem că este dată o *acțiune la stînga a lui G pe X* (sau că grupul G *acționează la stînga pe X,* sau că X este o *G-mulțime*) dacă este definită o funcție $\varphi : G \times X \to X$, cu următoarele proprietăți (notăm cu *gx elementul* $\varphi(g, x) \in X$, $\forall g \in G$, $\forall x \in X$):

a) $(gh)x = g(hx)$, $\forall g, h \in G$, $\forall x \in X;$

b) $ex = x$, $\forall x \in X$.

Dacă se dă o funcție $\varphi : X \times G \to X$ (notăm cu *xg elementul* $\varphi(x, g) \in X$), astfel încît:

a') $x(gh) = (xg)h$, $\forall g, h \in G$, $\forall x \in X;$

b') $xe = x$, $\forall x \in X,$

spunem că grupul G *acționează la dreapta pe* X.

Dacă G acționează la stînga pe X, iar $g \in G$, fie $\varphi_g : X \to X$ aplicația dată de $\varphi_g(x) = gx$, $\forall x \in G$. Observăm că *φ_g este o bijecție*, deoarece avem, $\forall x \in G$, $x = (gg^{-1})x = g(g^{-1}x) = (\varphi_g \circ \varphi_{g^{-1}})(x)$, deci $\varphi_g \circ \varphi_{g^{-1}} = \mathrm{id}$ (la fel, $\varphi_{g^{-1}} \circ \varphi_g = \mathrm{id}$); astfel, $\varphi_{g^{-1}}$ este inversa lui φ_g. Acest fapt conduce la următoarea:

1.3 Observație. Notăm cu $S(X)$ grupul permutărilor mulțimii X (numit şi *grupul simetric* pe X), adică :

$$S(X) = \{\sigma : X \to X \mid \sigma \text{ bijecție}\}.$$

Operația cu care este înzestrat $S(X)$ este compunerea uzuală a funcțiilor: $\forall \sigma, \tau \in S(X)$, $(\sigma \circ \tau)(x) = \sigma(\tau(x))$, $\forall x \in X$.

A da o acțiune la stînga a lui G pe X revine la a da un morfism de grupuri $\lambda : G \to S(X)$.

Într-adevăr, dacă G acționează la stînga pe X, definim $\lambda : G \to S(X)$ prin $\lambda(g) = \varphi_g$, $\forall g \in G$. Am văzut mai sus că $\varphi_g \in S(X)$. A spune că λ este morfism este o altă formulare a proprietății a) din definiție. Reciproc, dacă $\lambda : G \to S(X)$ este morfism de grupuri, definim $gx = \lambda(g)(x)$, $\forall g \in G$, $\forall x \in X$. Se verifică imediat că se obține o acțiune la stînga a lui G pe X.

1.4 Observație. *A da o acțiune la dreapta a lui G pe X revine la a da un morfism de grupuri $\rho : G \to S(X)^{\mathrm{op}}$*, unde $S(X)^{\mathrm{op}} = (S(X), *)$ este grupul „opus” lui $S(X)$, adică mulțimea $S(X)$ înzestrată cu operația de compunere a funcțiilor „scrise la dreapta argumentului”: $(\sigma * \tau)(x) = \tau(\sigma(x))$, $\forall x \in X$. [91]

În continuare, vom considera acțiuni la *stînga*, cazul acțiunilor la dreapta fiind asemănător (cf. exercițiul **1**). Introducem următoarea terminologie, inspirată din interpretarea „dinamică” a acțiunilor grupale:

1.5 Definiție. Fie $(G,\cdot)$ un grup, X o mulțime pe care G acționează şi $x \in X$. Mulțimea:

$$\boldsymbol{O}_x = \{gx \mid g \in G\}$$

este numită *orbita* (sau *traiectoria*) lui x (sub acțiunea lui G). Elementul x se numeşte *fixat* de $g \in G$ (sau *punct fix al lui* g) dacă $gx = x$. Dacă $gx = x$, $\forall g \in G$ (echivalent, $\boldsymbol{O}_x$ are un singur element), x este numit *punct fix al acțiunii lui* G. Notăm cu $\mathrm{Fix}_G(X)$ mulțimea punctelor fixe ale acțiunii lui G pe X.

Pentru orice $x \in G$, definim *stabilizatorul lui x în G* (sau *grupul de izotropie al lui x în G*), $\mathrm{Stab}_G(x) := \{g \in G \mid gx = x\}$ (notat uneori şi G_x). Vom omite indicele G dacă nu este pericol de confuzie, scriind $\mathrm{Stab}(x)$.

---

[91] Această compunere a funcțiilor este naturală dacă se scrie $(x)\sigma$ în loc de $\sigma(x)$: avem $(x)(\sigma * \tau) = ((x)\sigma)\tau$.

1.6 Exemple. a) Fie R un inel comutativ şi n un număr natural, $n \geq 2$. Grupul S_n al permutărilor mulțimii $\{1, 2, \ldots, n\}$ acționează asupra mulțimii $R[X_1,\ldots, X_n]$ (inelul polinoamelor de n nedeterminate cu coeficienți în R), astfel :

$\forall \sigma \in S_n, \forall p(X_1,\ldots, X_n) \in R[X_1,\ldots, X_n], (\sigma p)(X_1,\ldots, X_n) := p(X_{\sigma(1)},\ldots, X_{\sigma(n)})$.

Punctele fixe ale acțiunii lui S_n sunt polinoamele simetrice. La Exemplul **1**, polinoamele listate reprezintă orbita lui $X_1X_2 + X_3X_4$ sub acțiunea lui S_4.

b) Orice grup G acționează asupra mulțimii G prin *translații la stînga*: $\forall g \in G, \forall x \in X$, $gx := gx$ (înmulțirea lui g cu x în grupul G). O altă acțiune a lui G pe G este prin *conjugare*: $\forall g \in G, \forall x \in X, g{*}x := gxg^{-1}$. De obicei, acțiunea prin conjugare se consideră *la dreapta* definindu-se $x^g := g^{-1}xg, \forall g \in G, \forall x \in G$. Un element $x \in G$ are orbita formată dintr-un singur element $(x) \Leftrightarrow x \in C(G)$ (centrul lui G, elementele care comută cu toate elementele lui G).

c) Iată un exemplu din teoria ecuațiilor diferențiale. Fie $u : \mathbb{R}^n \to \mathbb{R}^n$ o funcție cu proprietatea că, $\forall p \in \mathbb{R}^n$, problema Cauchy

$$x'(t) = u(x(t)), \quad x(0) = p \tag{1}$$

are o unică soluție $x_p : \mathbb{R} \to \mathbb{R}^n$. De pildă, o condiție suficientă ca u să satisfacă proprietatea cerută este ca u să fie lipschitziană pe $\mathbb{R}^n$ ($\exists\, C > 0$ astfel încît $\|u(x) - u(y)\| \leq C\|x - y\|$, $\forall x, y \in \mathbb{R}^n$). Pentru detalii, vezi, de exemplu, BARBU [1985].

Definim atunci acțiunea "$*$" a grupului $(\mathbb{R}, +)$ pe $\mathbb{R}^n$ prin: $t{*}p = x_p(t), \forall t \in \mathbb{R}, \forall p \in \mathbb{R}^n$.

Să verificăm că am definit o acțiune. Avem de arătat că $(t + s){*}p = t{*}(s{*}p), \forall s, t \in \mathbb{R}$, $\forall p \in \mathbb{R}^n$, adică $x_p(t + s) = x_{s*p}(t) = x_{x_p(s)}(t)$. Pentru s fixat, funcția $z(t) := x_p(t + s)$ este soluție a problemei

$$z'(t) = u(z(t)), \quad z(0) = x_p(s).$$

Dar soluția acestei probleme este unică şi am notat-o $x_{x_p(s)}(t)$. Deci avem egalitatea de funcții $x_{x_p(s)}(t) = z(t) = x_p(t + s)$.

Avem şi $0{*}p = x_p(0) = p, \forall\, p \in \mathbb{R}^n$.

O interpretare a acestei acțiuni este următoarea: problema (1) defineşte, pentru orice $p \in \mathbb{R}^n$, o *traiectorie* a unui punct material M în $\mathbb{R}^n$ care, la momentul $t = 0$, este în punctul p. Rezultatul acțiunii lui t asupra lui p este poziția punctului M la momentul t.

d) **Izometrii.** Acest exemplu este extrem de sugestiv în ilustrarea faptului că *grupurile sînt o măsură a simetriei*.

Fie (X, d) un spațiu metric. O funcție bijectivă $T: X \to X$ care „păstrează distanțele”, adică $\forall x, y \in X$, are loc $d(T(x), T(x)) = d(x, y)$, se numeşte *izometrie*.

Condiția de bijectivitate este importantă pentru a putea defini *grupul izometriilor lui X*, $\mathrm{Izom}(X) := \{T: X \to X \mid T \text{ izometrie}\}$. Mai general, pentru orice submulțime $Y \subseteq X$, se

definește *grupul de simetrie al lui Y,* $S(Y) := \{T: X \to X \mid T(Y) = Y\}$.[92] Există spații metrice şi aplicații care păstrează distanțele, dar nu sînt izometrii (vezi Exercițiile). Deci Izom(X) este un subgrup al grupului tuturor permutărilor lui X (o permutare este o bijecție definită pe X cu valori în X).

Luînd $X = \mathbb{R}^2$, cu distanța euclidiană, Izom($\mathbb{R}^2$) este un grup care conține cu siguranță *translațiile de vector oarecare*, *simetriile față de o dreaptă dată* şi *rotațiile în jurul unui punct dat*.

Fie $u \in \mathbb{R}^2$. Translația de vector u este funcția $T_u : \mathbb{R}^2 \to \mathbb{R}^2$, $T_u(v) = u + v$, $\forall v \in \mathbb{R}^2$.

Simetria față de dreapta d duce orice punct $P \in \mathbb{R}^2$ în „simetricul său față de dreapta d" (unicul punct $S_d(P)$ cu proprietatea că d este mediatoarea segmentului $PS_d(P)$).

Rotația de unghi α în jurul punctului C duce un punct oarecare P în punctul $P' = R_{C,\alpha}(P)$ cu proprietatea că $d(C, P) = d(C, P')$ şi unghiul orientat (în sens trigonometric) $\widehat{PCP'}$ are măsura α.

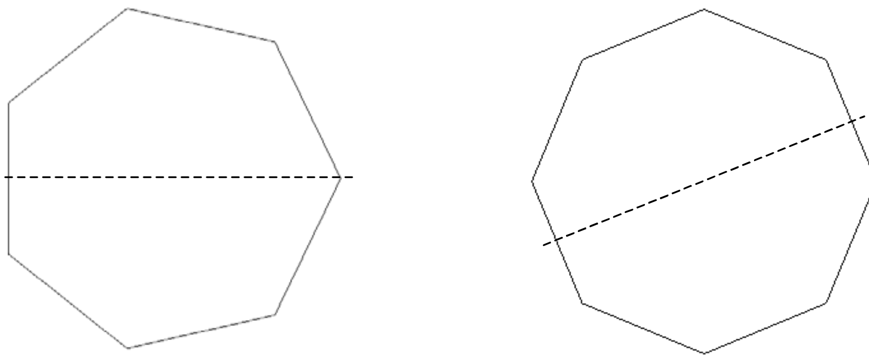
Observăm că izometria identitate este şi rotație (de unghi 0) şi translație (de vector 0). Are loc următoarea teoremă importantă:

O izometrie oarecare a planului este o translație urmată de o rotație şi eventual de o simetrie față de o dreaptă. (pentru demonstrație, vezi Exerciții)

Pentru teoria grupurilor este important grupul de simetrie al unui *poligon regulat cu n laturi*, numit grupul diedral D_n.

1.7 Propoziție. *Fie O centrul cercului circumscris unui poligon regulat cu n laturi. Grupul diedral D_n are* $2n$ *elemente şi este generat de rotația ρ de unghi $2\pi/n$ şi de simetria σ față de o axă de simetrie a poligonului* (o axă de simetrie a poligonului este o dreaptă ce uneşte centrul cercului circumscris cu un vîrf dacă *n este impar şi o mediatoare a unei laturi dacă n este par*). *Aceste izometrii satisfac relațiile* $\rho^n = \sigma^2 = \mathrm{id}$ *şi* $\sigma\rho = \rho^{n-1}\sigma$. □

Pentru detalii,vezi Exercițiile. Iată heptagonul regulat şi octogonul regulat, cu cîte o axă de simetrie:



[92] Arătați că Izom(X) este grup şi $S(Y)$ este subgrup al său.

Proprietăți elementare ale acțiunilor grupurilor pe mulțimi sînt colectate în:

1.8 Propoziție. *Fie G un grup care acționează pe o mulțime X. Atunci au loc afirmațiile:*

a) Definind $x \sim y \Leftrightarrow \exists g \in G$ *astfel încît* $y = gx$*, se obține o relație de echivalență pe X. Clasa de echivalență a unui element x este orbita lui x,* $\boldsymbol{O}_x$.

b) Pentru orice $x \in X$, $\mathrm{Stab}(x)$ *este un subgrup al lui G. Notînd cu* $G/_s\,\mathrm{Stab}(x)$ *mulțimea claselor la stînga ale lui G relativ la* $\mathrm{Stab}(x)$ *(adică* $\{g\cdot\mathrm{Stab}(x) \mid g \in G\}$*), aplicația* $\alpha : G/_s\,\mathrm{Stab}(x) \to \boldsymbol{O}_x$, $\alpha(g\cdot\mathrm{Stab}(x)) = gx$ $(\forall g \in G)$ *este bine definită și este o bijecție. În particular, avem*

$$|\boldsymbol{O}_x| = [G : \mathrm{Stab}(x)]$$

(cardinalul orbitei lui x este indicele stabilizatorului lui x în G).

c) Fie S un sistem de reprezentanți pentru orbitele lui G în X care au cel puțin 2 *elemente. Altfel spus, orice element din X este sau în* $\mathrm{Fix}_G(X)$*, sau în orbita unui unic element din S. Atunci*

$$X = \mathrm{Fix}_G(X) \cup \bigcup_{a\in S} \boldsymbol{O}_a \quad (\textit{reuniune disjunctă})$$

Trecînd la cardinali, rezultă relația:

$$|X| = |\mathrm{Fix}_G(X)| + \sum_{a\in S} [G : \mathrm{Stab}(a)]$$

Demonstrație. Exercițiu. □

Se pune problema calculării *numărului de orbite* al unei acțiuni.

1.9 Definiție. Pentru orice $g \in G$, notăm cu $\mathrm{Fix}(g) := \{x \in X \mid gx = x\}$ mulțimea acelor $x \in X$ fixați de g. Mai general, dacă $T \subseteq G$, punem $\mathrm{Fix}(T) = \{x \in X \mid gx = x, \ \forall g \in T\}$. Observăm că $\mathrm{Fix}(g) = \mathrm{Fix}(< g >)$, unde $< g >$ este subgrupul generat de g.

1.10 Propoziție. (*Lema lui Burnside*) *Fie G un grup finit care acționează pe o mulțime finită X. Atunci numărul k al orbitelor în X sub acțiunea lui G este „numărul mediu de puncte fixate” :*

$$k = \frac{1}{|G|}\sum_{g\in G} |\mathrm{Fix}(g)|.$$

Demonstrație. Considerăm mulțimea $M := \{(g, x) \in G \times X \mid gx = x\}$. Calculăm $|M|$.

Observăm că $(g, x) \in M \Leftrightarrow g \in \mathrm{Stab}(x)$; deci $M = \bigcup_{x\in X} \mathrm{Stab}(x) \times \{x\}$ (reuniune disjunctă). Astfel,

$$|M| = \sum_{x\in X} |\,\mathrm{Stab}(x)| = \sum_{x\in X} \frac{|G|}{[G : \mathrm{Stab}(x)]} = \sum_{x\in X} \frac{|G|}{|\boldsymbol{O}_x|}.$$

Însă X este reuniunea disjunctă a celor k orbite în X sub acțiunea lui G (fie acestea $T_1, \ldots, T_k$); putem scrie în continuare:

$$|M| = \sum_{i=1}^{k}\sum_{x\in T_i}\frac{|G|}{|\boldsymbol{O}_x|} = \sum_{i=1}^{k}\sum_{x\in T_i}\frac{|G|}{|T_i|} = \sum_{i=1}^{k}|G| = k\cdot|G|.$$

Pe de altă parte, $\forall g \in G$, $(g, x) \in M \Leftrightarrow x \in \mathrm{Fix}(g)$, deci $M = \bigcup_{g\in G} \{g\} \times \mathrm{Fix}(g)$ (reuniune disjunctă), deci:

$$|M| = \sum_{g\in G}|\mathrm{Fix}(g)|.$$

Comparînd cele două expresii pentru $|M|$, obținem formula. □

Aplicații

a) „Problema coroanei”. Fie $m, n \in \mathbb{N}$. Se consideră o coroană cu m vîrfuri (vîrfurile coroanei sînt vîrfurile unui poligon regulat cu m laturi). Se dau perle de n culori, în cantități suficiente. Cîte modele de coroană distincte se pot crea atașînd perle în fiecare vîrf al coroanei?

Soluție. În fiecare din cele m vîrfuri putem pune n culori, ceea ce dă n^m posibilități. Dar acesta nu e răspunsul corect: două astfel de configurații dau coroane identice dacă se obțin una din alta printr-o rotație a coroanei.

Traducem problema în termeni de *acțiuni ale grupurilor pe mulțimi*.

Se consideră X mulțimea colorărilor cu n culori a vîrfurilor unui poligon regulat cu m laturi, de centru O. Considerăm $X = \{(c_0, \ldots, c_{m-1}) \mid c_i \in \{1, 2, \ldots, n\}\}$; c_i este "culoarea vîrfului i". Fie R_m grupul rotațiilor planului (în jurul lui O) de unghiuri multiplu de $2\pi/m$. R_m este un grup ciclic cu m elemente, $R_m = \{r_0, r_1, \ldots, r_{m-1}\}$ unde r_k este rotația de unghi $2k\pi/m$.

G acționează asupra lui X. Cu notațiile de mai sus, avem $r_{-k}(c_0, \ldots, c_{m-1}) = (c_k, \ldots, c_{m-1+k})$ (indicii se consideră modulo m, adică $c_t = c_i$, $\forall t \in \mathbb{Z}$, unde i este restul împărțirii lui t la m).

Două colorări dau aceeași coroană dacă și numai dacă sînt în aceeași orbită a acestei acțiuni. Deci numărul orbitelor lui R_m în X este numărul cerut.

Pentru a găsi numărul de orbite, aplicăm lema lui Burnside. Fie $r_k \in R_m$; calculăm $|\mathrm{Fix}(r_k)|$.

Fie $d = (k,m)$; atunci $< r_k > = < r_d >$ (demonstrați!). Cum $\mathrm{Fix}(r_k) = \mathrm{Fix}(< r_k >) = \mathrm{Fix}(< r_d >) = \mathrm{Fix}(r_d)$, calculăm $|\mathrm{Fix}(r_d)|$. Dacă $(c_0, \ldots, c_{m-1})$ este o colorare invariată de r_d, atunci $c_0 = c_d = c_{2d} = \ldots = c_{id}$, $\forall i \in \mathbb{Z}$; în general, fixarea unei culori a unui vîrf determină culorile a m/d vîrfuri. Astfel, putem alege d vîrfuri distincte pe care să le colorăm arbitrar (de ex. $c_0, \ldots, c_{d-1}$), culorile celelalte fiind determinate de faptul că $(c_0, \ldots, c_{m-1})$ este o colorare invariată de r_d. Sînt $n^d = n^{(k,\, m)}$ posibilități de colorare, deci $|\mathrm{Fix}(r_k)| = n^{(k,\, m)}$. Formula lui Burnside dă numărul de orbite:

$$\frac{1}{m}\sum\nolimits_{k=1}^{m} n^{(k,m)}$$

Propunem cititorului să trateze direct (fără a folosi formula de mai sus) cazul $m = 5$, $n = 3$.

b) „Problema colierului”. Fie $m, n \in \mathbb{N}$. Cîte coliere distincte formate din m perle de n culori se pot fabrica? Se presupune că există suficiente perle de fiecare culoare.

Indicație. Aici acționează grupul diedral D_m (al simetriilor unui poligon regulat cu m laturi) asupra mulțimii X a colorărilor (colierul poate fi și „întors”, spre deosebire de coroană). D_m

are ca subgrup grupul R_m al rotațiilor, dar conține și reflecții față de drepte care trec prin centrul O. Se disting cazurile m par și m impar.

c) În cîte moduri se poate scrie 1000 ca un produs de trei numere naturale (la un produs dat nu contează ordinea factorilor)?

Exerciții

1. Fie $(G, \cdot)$ un grup și $(G^{op}, *)$ grupul opus lui G, adică mulțimea G înzestrată cu operația $x*y := y\cdot x$, $\forall x, y \in G$. Arătați că $(G^{op}, *)$ este grup și că a da o acțiune la stînga a lui G pe o mulțime X este echivalent cu a da o acțiune la dreapta a lui G^{op} pe X.

2. Fie M mulțimea șirurilor reale mărginite. Arătați că M este un spațiu liniar normat în raport cu norma $\|(x_n)_{n\geq 1}\| = \sup\{\, |x_n| \mid n \geq 1\}$. Dați exemplu de funcție $\varphi : M \to M$ care păstrează norma (deci și distanțele), dar care nu este bijecție.

3. Fie T o izometrie a planului. Demonstrați că:

a) T duce dreapta AB în dreapta $T(A)T(B)$.

b) Dacă T are trei puncte necoliniare fixe, atunci T este identitatea. Deduceți că o izometrie este determiunată de imaginile a trei puncte necoliniare.

c) Dacă T are două puncte fixe A și B și $T \neq \mathrm{id}$, atunci T este simetria față de dreapta AB.

d) Dacă T are exact un punct fix O, atunci T este o rotație în jurul lui O.

4. Două figuri plane (submulțimi ale planului) X și Y se numesc *congruente* dacă există o izometrie T a planului astfel încît $Y = T(X)$. Arătați că, dacă X și Y sînt congruente, atunci grupurile lor de simetrie sînt izomorfe. Reciproca este adevărată?

5. Fie X un spațiu metric și $Y \subseteq X$, $|Y| = n$. Atunci grupul de simetrie $S(Y)$ este izomorf cu un subgrup al grupului simetric S_n (grupul permutărilor de n obiecte).

6. Fie O centrul cercului circumscris unui poligon regulat cu n laturi $A_0A_1\ldots A_{n-1}$ și φ o izometrie din grupul său de simetrie D_n. Demonstrați că:

a) $\forall i,\ 0 \leq i \leq n-1$, are loc $\varphi(O) = O$ și $\varphi(A_i) \in \{A_0, A_1,\ldots, A_{n-1}\}$. Deduceți că D_n este un subgrup în S_n.

b) φ este determinat de imaginile a două vîrfuri consecutive. În plus, dacă $\varphi(A_0) = A_i$, atunci $\varphi(A_1)$ este unul din vîrfurile adiacente cu A_i.

c) Deduceți că D_n are cel mult $2n$ elemente.

d) Fie ρ rotația de unghi $2\pi/n$ în jurul lui O și σ simetria față de o axă de simetrie a poligonului. Atunci elementele : id, $\rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \rho\sigma, \rho^2\sigma, \ldots, \rho^{n-1}\sigma$ sînt distincte.

e) Scrieți tabla operației grupului D_n.

Index

D

E

F

G

I

L

M

N

O

P

R

S

Bibliografie

1. ALBU, T., ION, I.D. [1984] *Capitole de teoria algebrică a numerelor,* Ed. Academiei R.S.R., Bucureşti.
2. ALBU, T., ION, I.D. [1997] *Itinerar elementar în algebra superioară,* Ed. All, Bucureşti.
3. ALBU, T., MANOLACHE, N. [1987] *19 Lecţii de teoria grupurilor,* Ed. Universităţii Bucureşti, Bucureşti.
4. ALBU, T., RAIANU, Ş. [1984] *Lecţii de algebră comutativă,* Ed. Universităţii Bucureşti, Bucureşti.
5. ANDERSON, F.W., FULLER, K.R. [1974] *Rings and categories of modules,* Springer-Verlag, New York.
6. AYAD, M. [1997] *Théorie de Galois. 122 exercices corrigés*, Ellipses, Paris.
7. BARBU, V. [1985] *Ecuaţii diferenţiale*, Ed. Junimea, Iaşi.
8. BECHEANU, M. et al. [1983], *Algebră pentru perfecţionarea profesorilor,* Ed. didactică şi pedagogică, Bucureşti.
9. BOREVICI, Z.I, ŞAFAREVICI, I.R. [1985], *Teoria numerelor,* Ed. Ştiinţifică şi Enciclopedică, Bucureşti.
10. BOURBAKI, N. [1958] *Eléments de mathématique*, Fasc. VII, Livre II: *Algèbre*, Chapitre 3, *Algèbre multilinéaire*, Hermann, Paris.
11. BOURBAKI, N. [1967] *Eléments de mathématique*, Fasc. VI, Livre II: *Algèbre*, Chapitre 2, *Algèbre linéaire*, Hermann, Paris.
12. BOURBAKI, N. [1981] *Algèbre*, Chapitres 4 à 7, Masson, Paris.
13. BOURBAKI, N. [1985] *Eléments de mathématique*: *Algèbre commutative*, Chapitres 1 à 4, Masson, Paris.
14. ESCOFIER, J.P. [1997] *Théorie de Galois*, Masson, Paris.
15. FRIED, M., JARDEN, M. [1986], *Field Arithmetic*, Springer Verlag, Berlin.
16. FREUDENTHAL, H. [1973], *Limbajul logicii matematice,* Ed. Tehnică, Bucureşti.
17. GEDDES, K., CZAPOR, S., LABAHN, G. [1992], *Algorithms for Computer Algebra*, Kluwer Academic Publishers.
18. GOZARD, I. [1997] *Théorie de Galois*, Ellipses, Paris.
19. HALL, M. [1959] *The Theory of Groups*, Macmillan, New York.
20. HUNGERORD, T.W. [1974], *Algebra,* Springer-Verlag, New York.

21. ION, I.D., NĂSTĂSESCU, C., NIȚĂ, C. [1984] *Complemente de algebră*, Ed. Ştiinţifică şi enciclopedică, Bucureşti.
22. ION, I.D., RADU, N. [1981a] *Algebra*, Ed. Didactică şi pedagogică, Bucureşti.
23. ION, I.D., RADU, N., NIȚĂ, C., POPESCU, D. [1981b] *Probleme de algebră*, Ed. Didactică şi pedagogică, Bucureşti.
24. JACOBSON, N. [1964], *Lectures in Abstract Algebra III. Theory of Fields and Galois Theory*, Springer-Verlag, New York.
25. JACOBSON, N. [1974], *Basic Algebra I*, W.H. Freeman and Co., San Francisco.
26. KAPLANSKY, I. [1973], *Fields and Rings*, The University of Chicago Press, Chicago.
27. KOSTRIKIN, A.I, SHAFAREVICH, I.R. (Eds.) [1990] *Algebra I. Basic Notions of Algebra* (I.R. SHAFAREVICH), Encyclopaedia of Mathematical Sciences, vol. 11, Springer Verlag.
28. LAFON, J.P. [1977] *Algèbre commutative. Langages géometrique et algébrique*, Hermann, Paris.
29. LINT, J.H. VAN [1982], *Introduction to Coding Theory*, Springer-Verlag, New York.
30. MACCARTHY, P.J. [1966], *Algebraic Extensions of Fields*, Blaisdell Publishing, Waltham, Massachusets.
31. MANIN, YU. I. [1977], *A Course in Mathematical Logic*, Springer Verlag, New York.
32. MARINESCU, GH. [1983], *Analiză matematică, vol. I* , Ed. Academiei R.S.R., Bucureşti.
33. MORANDI, P. [1996] *Field and Galois Theory*, Springer-Verlag, New York.
34. NĂSTĂSESCU, C. [1974] *Introducere în teoria mulțimilor*, Ed. Didactică şi pedagogică, Bucureşti.
35. NĂSTĂSESCU, C. [1976] *Inele. Module. Categorii*, Ed. Academiei R.S.R., Bucureşti.
36. NĂSTĂSESCU, C., NIȚĂ, C. [1979] *Teoria calitativă a ecuațiilor algebrice*, Ed. Tehnică, Bucureşti.
37. NĂSTĂSESCU, C., NIȚĂ, C., VRACIU, C. [1986] *Bazele Algebrei, vol. I*, Ed. Academiei R.S.R., Bucureşti.
38. NĂSTĂSESCU, C. [1983] *Teoria dimensiunii în algebra necomutativă,* Ed. Academiei R.S.R., Bucureşti.
39. NEUKIRCH, J. [1986] *Class Field Theory*, Springer-Verlag, Berlin.
40. NIȚĂ, C., SPIRCU, T. [1974] *Probleme de structuri algebrice*, Ed. Tehnică, Bucureşti.
41. PARENT, D.P. [1978] *Exercices en théorie des nombres,* Gauthier-Villars, Paris.
42. POPESCU, N. [1971] *Categorii abeliene*, Ed. Academiei R.S.R., Bucureşti.
43. PURDEA, I. [1982] *Tratat de algebră modernă,* vol II, Ed. Academiei R.S.R., Bucureşti.
44. RADU, GH. [1988] *Algebra categoriilor şi functorilor*, Ed. Junimea, Iaşi.
45. RADU, N. [1968] *Inele locale,* vol. I, Ed. Academiei R.S.R., Bucureşti.
46. REGHIȘ, M. [1981] *Elemente de teoria mulțimilor şi logică matematică*, Ed. Facla, Timişoara.
47. SAMUEL, P. [1963] *Anneaux factoriels*, Sociedade de Matemática de São Paulo.

48. SAMUEL, P. [1968] *Théorie algébrique des nombres*, Hermann, Paris.
49. SCORPAN, A. [1996] *Introducere în teoria axiomatică a mulțimilor*, Ed. Universității București, București.
50. SIREȚCHI, GH. [1978] *Analiză matematică, vol. I*, ed IV., Tipografia Univ. București.
51. SHPARLINSKI, I., [2003] *Cryptographic applications of analytic number theory. Complexity lower bounds and pseudorandomness*, Progress in Computer Science and Applied Logic, 22. Birkhäuser Verlag, Basel.
52. SPINDLER, K. [1994] *Abstract Algebra with Applications*, *vol. I, II,* M. Dekker, New York.
53. ȘTEFĂNESCU, M., [1993] *Introducere în teoria grupurilor,* Ed. Universității „Al. I. Cuza", Iași.
54. TEODEORESCU, P.P., NICOROVICI-PORUMBARU, N. [1985], *Aplicații ale teoriei grupurilor în mecanică și fizică,* Ed. Tehnică, București.
55. TIGNOL, J.-P. [1987] *Galois' Theory of Algebraic Equations,* Longman Scientifical and Technical.
56. WINKLER, F. [1996], *Polynomial Algorithms in Computer Algebra,* Springer Verlag Wien-NewYork.
57. VAN DER WAERDEN, B.L. [1967], *Algebra II* (Fünfte auflage der Modernen Algebra) Springer-Verlag, Berlin.
58. VAN DER WAERDEN, B.L. [1971], *Algebra I* (Achte auflage der Modernen Algebra) Springer-Verlag, Berlin.
59. VAN DERWAERDEN, B.L. [1985], *A History of Algebra,* Springer-Verlag, Berlin.
60. WALKER, R.J. [1950] *Algebraic Curves*, Dover Publications, New York.